Universidad Nacional Autónoma de Nicaragua, Managua
(UNAN-Managua)
Recinto Universitario Rubén Darío
(RURD)
Facultad de Educación e Idiomas
Departamento de Francés

Carrera: Traducción e Interpretación Francesa

Trabajo de Seminario para optar al Título de Licenciatura en Traducción e Interpretación Francesa

Tema: Desafíos y estrategias para la traducción del texto de Matemática Álgebra y Teoría de Números de L. Koulikov y sus posibles soluciones

Tutora: Ángela Munguía Beteta

Integrantes:

- **Adrian Daniel García Flores**
- **Xochilt Beatriz Arauz Cárcamo**
- **Keren Rebeca Cerrato Hernández**
- **Adriana Carmen Flores Gavarrete**
- **Amelia Hernández Hernández**
- **Francisco Guillermo Rocha Martínez**
- **Raisa Irina Sevilla Guevara**
- **Christian Patricia Cano Méndez**
- **Tania Alejandra Perez Luna**
- **Gaudy Junieth Ruiz Bonilla**
- **Jonathan Blessing Martínez Bravo**
- **Ingrid Valeria Largaespada Hernández**
- **Sonia Mercedes Ardila Gutiérrez**
- **Nelson Enrique Mendoza Rugama**

PRÓLOGO

Estos últimos años se introdujo en los institutos pedagógicos un nuevo plan de estudios unificado de álgebra y teoría de números. El objetivo principal de este curso es el estudio de los sistemas algebraicos fundamentales así como la formación en cultura algebraica de los futuros docentes, necesaria para la comprensión profunda de los objetivos y tareas de un curso escolar de matemáticas básicas u optativas. El libro propuesto se redactó de acuerdo a los nuevos programas.

De manera convencional el libro se puede dividir en tres partes íntimamente ligadas. La primera parte presenta elementos de lógica, conceptos sobre conjuntos y relaciones, nociones preliminares sobre álgebras y sistemas algebraicos, sistemas numéricos de base. Los elementos de lógica y teoría de conjunto se describen de manera muy completa y son ampliamente utilizados en el curso de álgebra y otras ramas de las matemáticas. La información preliminar sobre las álgebras y sistemas algebraicos, grupos y anillos se expone en el capítulo III. Sobre esta base se estudiaron los sistemas numéricos fundamentales: sistema de números naturales, anillo de enteros, cuerpo de números racionales, sistema de números reales y cuerpo de números complejos. El sistema de números reales se introduce como un cuerpo totalmente completo ordenado (arquimediano). La segunda parte (capítulos V – IX) se destinan al álgebra lineal. Primeramente se estudian los espacios vectoriales aritméticos y los sistemas de ecuaciones lineales, exceptuando los determinantes. El capítulo VI es el único en el que los determinantes se aplican a la solución de sistemas de ecuaciones lineales. Esta manera no tradicional de proceder aligera el cálculo de los problemas principales, la teoría de sistema de ecuaciones lineales que así se incorporan orgánicamente a la teoría de espacios vectoriales aritméticos. El capítulo IX trata los sistemas de desigualdades lineales y los elementos de programación lineal (problemas canónicos y problemas estándares, principio de dualidad y método de simplex).

La tercera parte del libro (capítulos X-XVII) se dedica a los grupos, análisis numéricos y teóricos, anillos, anillos de polinomios. En los últimos dos capítulos se estudian los anillos de polinomios asociados a los cuerpos numéricos de base así como los elementos de la teoría de los cuerpos.

Muchos capítulos vinculan estrictamente a los nuevos programas escolares y pueden servir de base en las asignaturas optativas.

Todos los capítulos se dividen en párrafos. Si se refiere al párrafo de un capítulo, solamente se indica el número del párrafo. En la referencia del párrafo de otro capítulo el número del capítulo precede al del párrafo citado. Los teoremas, proposiciones y corolarios de un mismo párrafo se enumeran sucesivamente. La referencia del teorema o la propuesta del capítulo se muestran al indicar el número de párrafo seguido del teorema. La referencia al teorema o a la propuesta de otro capítulo contiene sucesivamente el número del capítulo, del párrafo y del teorema. Por ejemplo, la referencia “teorema 4.2” significa teorema 2 del párrafo 4 del mismo capítulo, “teorema 4.2.6” teorema 6 del párrafo 2 del capítulo IV.

El autor agradece afectuosamente a los profesores B.M. Brédikhine y M.M. Gloukhov por sus análisis y comentarios críticos que hicieron posible la mejora del manuscrito de este libro.

PRIMER CAPÍTULO
ELEMENTOS DE LÓGICA

§ 1. Lógica de afirmaciones

Afirmaciones. La noción de "afirmación" es primaria. Se entiende en lógica por afirmación al enunciado de una proposición de la que se puede decir que es verdadera o bien, falsa. Toda afirmación, sea verdadera o falsa pero ninguna verdadera y falsa a la vez.

Ejemplos de afirmaciones: $\ll 0 < 1 \gg$, $\ll 2 \cdot 3 = 6 \gg$, "5 es un número par, "1 es un número primo". El valor de verdad de las dos primeras afirmaciones es "verdadero", el valor de verdad de las dos últimas es "falso".

Las proposiciones interrogativas y exclamativas no son afirmaciones. Una definición no es una afirmación. Por ejemplo, la definición "un número entero es par si es divisible por 2" no es una afirmación. En cambio, el enunciado de la proposición "si un número entero es divisible por 2 entonces es par" constituye una afirmación que además es verdadera. La lógica de afirmaciones hace abstracción del sentido lógico de la afirmación y se goza de responder sin ambigüedad a la pregunta: ¿El enunciado de la proposición es verdadero o falso?

En seguida de lo expuesto entenderemos por sentido de la afirmación su valor de verdad (la afirmación ¿es ≪verdadera≫ o ≪falsa≫?). Las afirmaciones se notaran por mayúsculas latinas, mientras que sus valores, es decir si son verdaderas o falsas, por las letras V o F respectivamente.

La lógica de afirmaciones estudia las relaciones que se determinan de manera exhaustiva mediante procedimientos que permitan formar otras afirmaciones a partir de afirmaciones dichas elementales. Las afirmaciones elementales se consideran como enteras, indivisibles en partes, su estructura interna no nos interesa.

Operaciones lógicas sobre afirmaciones. A partir de las afirmaciones elementales, mediante operaciones lógicas, se puede obtener nuevas afirmaciones, más complicadas. El valor de la verdad de la afirmación compleja es función de los valores de verdad que forman la afirmación compleja. Esta dependencia se establece mediante definiciones dadas más adelante, y se constataran construyendo tablas de verdad. En las columnas de la izquierda de estas tablas se indican las disposiciones posibles de valores de verdad de afirmaciones que forman una afirmación compleja considerada. En la columna derecha se escriben los valores de verdad de la afirmación compleja que corresponden a las distribuciones de cada línea.

Sean A y B dos afirmaciones cualesquiera sobre los valores de verdad de los que se abstienen de hacer hipótesis. Se denomina *negación de la afirmación* A la nueva afirmación verdadera si y sólo si A es falsa. La negación A se denota $\neg A$ y se lee "no A" o "negación de A". La operación de negación se deduce por la tabla de verdad.

A	$\neg A$
V	F
F	V

Ejemplo. La afirmación "es falso que 5 es un número par" cuyo valor es V, la negación de la falsa afirmación "5 es un número par".

Con ayuda de la operación de conjunción se forma a partir de dos afirmaciones una compleja denotada $A \wedge B$. Por definición, la afirmación $A \wedge B$ es verdadera si y solo si las dos afirmaciones A y B son verdaderas. Las afirmaciones A y B son respectivamente denominadas primer y segundo miembro de la conjunción $A \wedge B$. La notación "$A \wedge B$" se lee "A y B". La tabla de verdad de la conjunción es de la forma

A B	$A \wedge B$

V V	V
V F	F
F V	F
F F	F

Ejemplo. La afirmación "7 es un número primo y 6 un número impar" es falsa, como conjunción de dos afirmaciones de las que una es falsa.

Se denomina disyunción a dos afirmaciones A y B la afirmación denotada $A \vee B$ si y solo si una de las dos afirmaciones es verdadera. Respectivamente, la afirmación $A \vee B$ es falsa sí y sólo sí A y B son las dos falsas. Las afirmaciones A y B son igualmente denominadas primer y segundo miembro de la disyunción $A \vee B$. Se lee la notación $A \vee B$ "A o bien B". La conjunción "o" tiene en este caso un sentido no exclusivo, ya que la afirmación $A \vee B$ es verdadera si los dos miembros son verdaderos. La disyunción se puede presentar bajo la forma de tabla de verdad siguiente:

$A\ B$	$A \vee B$
$V\ V$	V
$V\ F$	V
$F\ V$	V
$F\ F$	F

Ejemplo. La afirmación " $3 < 8\ o\ 5 < 2$" es una disyunción de dos afirmaciones de la que una es verdadera y su valor es V.

La afirmación denotada $A \rightarrow B$, falsa sí y sólo sí A es verdadera, mientras B es falsa, se denominan *implicación* con premisa A y conclusión B. La afirmación $A \rightarrow B$ se lee "si A, entonces B" o bien "A implica B" igualmente "de A se deduce B". La tabla de verdad de implicación es de la forma

$A\ B$	$A \rightarrow B$
$V\ V$	V
$V\ F$	F
$F\ V$	V
$F\ F$	V

Fíjese que entre la premisa y la conclusión puede no existir relación de causa y efecto, de todas maneras este hecho no valida la veracidad o la falsedad de la implicación. Por ejemplo, la afirmación "si 5 es un número primo, la bisectriz de un triángulo isósceles es una mediana" es verdadera de acuerdo al sentido común la segunda afirmación no se deriva de la primera. Sera igualmente verdadera la afirmación "si $2 + 2 = 5$, entonces $6 + 3 = 9$", ya que su conclusión es verdadera. Con esta definición si la conclusión es verdadera, la implicación será verdadera sea cual sea el valor de verdad de la premisa. En el caso en el que la premisa sea falsa, la implicación será verdadera independientemente del valor de verdad de la conclusión. Esta circunstancia se establece someramente así: "la verdad puede provenir de todo", "todo puede provenir de una afirmación falsa"

La afirmación denotada $A \leftrightarrow B$, es verdadera sí y sólo sí A y B tienen el mismo valor de verdad, es denominada *equivalencia.* La afirmación $A \leftrightarrow B$ se lee "A sí y sólo sí B" o "A es equivalente a B" o también "A es una condición necesaria y suficiente para que B tenga lugar". La tabla de verdad para equivalencia es de la forma.

$A\ B$	$A \leftrightarrow B$
$V\ V$	V
$V\ F$	F
$F\ V$	F
$F\ F$	V

Ejemplo: La afirmación " $2 > 5$ sí y sólo sí $3 + 0 = 4$" es verdadera como equivalencia de dos afirmaciones falsas.

Fórmulas de la lógica de afirmaciones. El objetivo principal de la lógica de afirmaciones es el estudio de formas lógicas de las afirmaciones complejas mediante operaciones lógicas. La noción de forma lógica de la afirmación compleja se esclarece por la introducción de la noción de fórmula de la lógica de afirmaciones hecha más adelante.

Para la notación de afirmaciones se utilizará minúsculas latinas del fin del alfabeto (si se necesita con índices). Por hipótesis se ignora en este caso cual afirmación (verdadera o falsa) se designa por tal o tal letra. En efecto, las letras

(1) $p, q, r, \dots\ ,\ p_1, q_2,$

Serán variables que adquieren a modo de valores los valores de verdad "verdadero" y "falso". Generalmente, estas variables son denominadas *variables proposicionales*; se les llamara igualmente *fórmulas elementales* o *átomos.*

Para las fórmulas de lógica de afirmaciones se utilizan además de los símbolos (1) signos de operación lógica

¬ , ∧ , ∨, → , ↔

Al igual que los símbolos que garantizan una lectura univalente de las fórmulas – paréntesis izquierda y derecha: (,).

Preséntese la noción de *fórmula de la lógica de afirmaciones* de la manera siguiente:

1) Las fórmulas elementales (los átomos) constituyen fórmulas de la lógica de afirmaciones;
2) Si A y B son fórmulas, $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ son igualmente fórmulas de la lógica de afirmaciones;
3) Solo las expresiones que constituyen inferencias de 1) y 2) son fórmulas de la lógica de afirmaciones.

La definición de la fórmula implica la enumeración de reglas de composición de fórmulas. Según la definición toda fórmula de la lógica de afirmaciones es, ya sea un átomo, una expresión formada de átomos y obtenida por la aplicación seguida de la regla 2). Por ejemplo, las expresiones

$$p, (\neg q), \big((r \vee s) \rightarrow t\big), ((p \vee (\neg p)) \leftrightarrow (p \rightarrow q)$$

Son fórmulas de la lógica de afirmaciones.

Se notara las fórmulas arbitrarias de la lógica de afirmaciones por medio de mayúsculas latinas (afectadas si necesita de índices):

$$A, B, C, \qquad \dots A_1, B_1, C_1, \dots$$

Igualmente no se excluye que la misma fórmula pueda expresarse por letras diferentes.

Nótese que ningún átomo puede representarse bajo la forma,
$(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$. Es el aspecto que pueden adquirir las fórmulas complejas.

En el primer capítulo en lugar de "formula de la lógica de afirmaciones" se dirá simplemente "formula" ahí donde no conlleve a ninguna equivocación.

El número de paréntesis se puede reducir estableciendo el acuerdo: 1) en una formula compleja se eliminara los dos paréntesis exteriores; 2) se ordenan los signos de operaciones lógicas siguiendo el orden de prioridad dada: signos. En esta sucesión de signos, el signo ↔ tiene el dominio de acción más largo, en cambio el signo ¬ el más restringido. Se entiende por dominio de acción del signo de operación a las partes de la fórmula a las cuales se "aplica" (sobre las que "interviene") el signo introducido considerado. No conviene encerrar en paréntesis las partes de las fórmulas que se pueden tomar en cuenta por la jerarquía de la fuerza acumulada. Restituyendo los paréntesis introducimos primero las partes que llevan el signo ¬ (yendo de izquierda a derecha) seguido de las partes que llevan el signo ∧ , etc.
Ejemplo. En la fórmula $B \leftrightarrow \neg C \vee D \wedge A$ los paréntesis se restituyen de la siguiente manera:

$B \leftrightarrow (\neg C) \vee D \wedge A$, $\quad B \leftrightarrow \big((\neg C \vee D \wedge A)\big)$,

$B \leftrightarrow (\neg C) \vee (D \wedge A)$, $\quad \Big(B \leftrightarrow \big((\neg C) \vee (D \wedge A)\big)\Big)$.

No se puede privar de paréntesis a toda la fórmula. Por ejemplo en las fórmulas
$A \rightarrow (B \rightarrow C), \neg(A \rightarrow B)$ es imposible ejecutar una subsecuente eliminación de paréntesis.

Leyes lógicas. Existen fórmulas que se mantienen válidas (son verdaderas) independientemente de los valores del contenido de átomos que las forman. Por ejemplo

$$A \vee \neg A, A \rightarrow A, (A \rightarrow B) \vee (B \rightarrow A), A \rightarrow (B \rightarrow A)$$

Estas fórmulas juegan un rol particular en lógica.

DEFINICIÓN. Una fórmula de la lógica de afirmaciones que adquiere el valor "verdadero" por toda distribución de valores atómicos que constituyen la fórmula se dice *siempre verdadera, tautológica* o *ley lógica.*

Existen fórmulas no válidas (es decir, falsas) sea cual sean los valores de los átomos que constituyen. Por ejemplo,

$A \wedge \neg A$, $(A \vee \neg A) \rightarrow (A \wedge \neg A)$.

DEFINICIÓN. Una fórmula de la lógica de afirmaciones que queda falsa por toda distribución de valores atómicos que constituye la fórmula se dice *siempre falsa* o *contradicción.*

Es fácil convencerse de que si A es una contradicción, $\neg A$ será una tautología y viceversa. Por ejemplo, la formula $p \wedge \neg p$ siempre es falsa, mientras que $\neg(p \wedge \neg p)$ es una tautología.

Existen fórmulas que toman ya sea el valor "verdadero" o el "falso" siguiendo los valores que adquieren los átomos que figuran. Por ejemplo,

$A \vee A$, $A \rightarrow B$, $A \wedge B \rightarrow B \wedge C$.

La notación $\vDash A$ significa que A es una tautología; por ejemplo, $\vDash A \bigvee \neg\ A$. Esta ley lleva el nombre de *ley de terceros excluidos.*

TEOREMA 1.1 Si A y $(A \rightarrow B)$ *son tautologías*, B *también es una tautología.*

Demostración. Supóngase que A y $(A \to B)$ son tautologías. Admítase que por una distribución cualquiera de los valores de verdad de átomos formando A y B la fórmula B toma el valor "falso". Dado que A es una tautología, por una misma distribución de valores de verdad de los átomos, la fórmula A adquiere el valor "verdadero". Como resultado, la fórmula $(A \to B)$ es entonces falsa, lo que es contrario a la hipótesis según la cual $(A \to B)$ es una tautología. Por lo tanto, la fórmula B es V para toda distribución de valores de verdad de sus átomos. □*

TEOREMA 1.2 *Sea A una fórmula que contienen átomos p_1,…, p_n, mientras que B es una fórmula que se obtiene a partir de A sustituyendo al mismo tiempo a p_1,. . ., p_n las fórmulas A_1. . ., A_n respectivamente. Si A es una tautología, B lo es también.*

Demostración. Supóngase que dada una distribución cualquiera de valores de verdad de los átomos que componen B. Para esta distribución de valores de átomos las fórmulasA_1. . ., $A_n$tomaran respectivamente los valores de verdad a_1,…, a_n. Si se le da a los átomos p_1,. . ., $p_n$respectivamente los valores de a_1,…, a_n el valor de verdad de la formula A coincidirá entonces con el de la fórmula B por la distribución dada de los valores de los átomos que forman B. Dado que por hipótesis A es una tautología, para la distribución dada de los valores de átomos B tienen un valor "verdadero", es decir B también es una tautología. □

Este TEOREMA muestra que toda permutación en una tautología conduce a una tautología.
Más abajo (con el TEOREMA 1.3) se dan las leyes lógicas más frecuentes.

TEOREMA 1.3 Las fórmulas siguientes son tautologías: Implicaciones tautológicas

$p \wedge (p \to q) \to q$	*Ley de conclusión*
$p \wedge q \to p$	*Ley de eliminación de la conjunción.*
$p \wedge q \to q$	
$p \to p \vee q$	*Ley de inclusión de la disyunción.*
$q \to p \vee q$	
$(p \vee q) \wedge \neg q \to p$	*Ley de eliminación de la disyunción.*
$p \to \neg\neg\, p$	*Ley de la inclusión de la doble negación*
$\neg\neg\, p \to p$	*Ley de la eliminación de la doble negación*
$(p \to q) \wedge (q \to p) \to (p \leftrightarrow q)$	*Ley de inclusión de la equivalencia*
$(p \leftrightarrow q) \to (p \to q)$ $(p \leftrightarrow q) \to (q \to p)$	*Ley de eliminación de la equivalencia*
$(p \to q) \to (\neg q \to \neg p)$	*Ley de contraposición*
$(\neg p \to q) \wedge (\neg p \to \neg q) \to p$	*Ley de demostración a contrario*
$(p \to q) \wedge (q \to r) \to (p \to r)$	*Ley del silogismo*
$(p \to r) \wedge (q \to r) \to (p \vee q \to r)$	*Ley de adición de premisas*
$(p \to q) \wedge (p \to r) \to (p \to q \wedge r)$	*Ley del producto de conclusiones*

* El signo □ significa que la demostración del teorema o de la proposición está concluida.

$(p \leftrightarrow q) \wedge (q \leftrightarrow r) \rightarrow (p \leftrightarrow r)$	*Ley de la transitividad de la equivalencia.*

Equivalencias tautológicas:

$p \leftrightarrow p$	*Ley de identidad (de equivalencia lógica)*
$p \wedge p \leftrightarrow p$	*Ley de ídem potencia de la conjunción*
$p \vee p \leftrightarrow p$	*Ley de la ídem potencia de la disyunción*
$p \wedge q \leftrightarrow q \wedge p$	*Ley de la conmutatividad de la conjunción*
$p \vee q \leftrightarrow q \vee p$	*Ley de la conmutatividad de la disyunción*
$p \wedge (p \wedge r) \leftrightarrow (p \wedge q) \wedge r$	*Ley de la asociación de la conjunción*
$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$	*Ley de la asociación de la disyunción*
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	*Ley de la distribución de la conjunción en relación a la disyunción*
$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	*Ley de la distribución de la disyunción relativa a la conjunción*
$\neg\neg p \leftrightarrow p$	*Ley de la doble negación*
$(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$	*Ley de la conmutatividad de la equivalencia*
$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$	*Ley de la contraposición*
$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$	*Ley de negación de la disyunción*
$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$	*Ley de negación de la conjunción*
$(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$	*Ley de contrarios*
$p \rightarrow (q \rightarrow r) \leftrightarrow q \rightarrow (p \rightarrow r)$	*Ley de permutación de premisas.*

Tautologías que traducen ciertas operaciones por medio de otras:

$p \rightarrow q \leftrightarrow \neg p \vee q$;

$p \rightarrow q \leftrightarrow \neg(p \wedge \neg q)$;

$p \vee q \leftrightarrow \neg p \rightarrow q$;

$p \vee q \leftrightarrow \neg(\neg p \wedge \neg q)$;

$p \wedge q \leftrightarrow \neg(p \rightarrow \neg q)$;

$p \wedge q \leftrightarrow \neg(\neg p \vee \neg q)$;

$(p \leftrightarrow q) \leftrightarrow (p \leftrightarrow q) \wedge (q \rightarrow p)$

Para demostrar que cada una de las fórmulas proporcionadas es una tautología es necesario recurrir al método de tablas de verdad, es decir construir para cada fórmula la tabla de verdad y asegurarse que sobre cada línea de la columna marginal de derecha figure la letra V.

A título de ejemplo tomemos la ley del silogismo:

p	q	r	$p \to q$	$q \to r$	$p \to r$	$(p \to q) \wedge (q \to r) \to (p \to r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	V
V	F	V	F	V	V	V
V	F	F	F	V	F	V
F	V	V	V	V	V	V
F	V	F	V	F	V	V
F	F	V	V	V	V	V
F	F	F	V	V	V	V

Nótese que en virtud las leyes de asociación es posible eliminar los paréntesis que encuadran el grupo de miembros formados de conjunciones y disyunciones poli nominales. A partir de la ley de la doble negación se deriva, si es necesario, que una sucesión de dos signos "¬¬" o más siempre se evita.

Ejercicios

1. Construir la tabla de verdad para cada una de las fórmulas

(a) $p \to q \leftrightarrow \neg p \vee q$;

(b) $p \to \neg(q \wedge r)$;

(c) $r \to (r \to q)$;

(d) $(p \wedge q) \to (s \wedge \neg\, s \to p \vee s)$.

2. ¿Qué se puede decir del valor "verdadero" de la afirmación $\neg A \wedge B \leftrightarrow A \vee B$ si el valor de la afirmación $A \rightarrow B$ es calificada falsa?

3. Demostrar que las fórmulas del TEOREMA 1.3 son tautologías.

4. Sea C una fórmula que implica una inclusión de la fórmula A, mientras que C' es la fórmula obtenida a partir de C al reemplazar esta inclusión de la fórmula A por la fórmula B. Demostrar que si $A \leftrightarrow B$ es una tautología, $C \leftrightarrow C'$ lo es igualmente.

5. ¿Cuantas líneas posee la tabla de verdad de la fórmula lógica de afirmaciones formadas de n átomos diferentes?

6. Supóngase que la formula A es construida a partir de átomos $p_{1,\dots}$, $p_n$únicamente con la ayuda de signos $\neg$, $\wedge$, $\vee$ y la fórmula A^* es obtenida a partir de A al reemplazar cada inclusión de $\wedge$ por el símbolo de $\vee$ y viceversa; remplazando cada inclusión p_i por la inclusión $\neg p_i$ y viceversa. Demostrar que la fórmula $\neg A \leftrightarrow A^*$ es una tautología.

7. Demostrar que las fórmulas siguientes son tautologías:

(a) $(A \wedge B) \rightarrow C \leftrightarrow A \rightarrow (B \rightarrow C)$;
(b) $(A \wedge B) \rightarrow C \leftrightarrow (A \wedge \neg C) \rightarrow \neg B$;
(c) $\neg(A \rightarrow B) \leftrightarrow A \wedge \neg B$;
(d) $(A \rightarrow B) \wedge \neg B \rightarrow \neg A$;
(e) $A \rightarrow (\neg A \rightarrow B)$;
(f) $A \rightarrow (B \rightarrow A)$;
(g) $(\neg A \rightarrow A) \rightarrow A$;
(h) $(A \rightarrow B) \rightarrow (A \wedge C \rightarrow B \wedge C)$;
(i) $(A \rightarrow B) \wedge (C \rightarrow D) \rightarrow (A \wedge C \rightarrow B \wedge D)$;
(j) $(A \rightarrow B) \wedge (C \rightarrow D) \rightarrow (A \vee C \rightarrow B \vee D)$;
(k) $\neg(A \leftrightarrow B) \leftrightarrow (\neg(A \rightarrow B) \vee \neg(B \rightarrow A))$

8. Mostrar que ninguna fórmula de la lógica de afirmaciones construida únicamente con los signos de operaciones lógicas $\wedge$, $\vee$ no constituyen ni una tautología, ni una contradicción.

§ 2. Deducción Lógica

Definiciones principales. Sean $A_{1,}. . .,\ A_m, B$ las fórmulas de la lógica de afirmaciones.

DEFINICIÓN. La fórmula B se denomina *deducción lógica de las fórmulas* $A_1, \dots, A_m$si con una elección cualquiera de valores de verdad de los átomos, que entra en las fórmulas $A_1, \dots, A_m$, B, la fórmula B adquiere el valor "verdadero" cada vez que cada una de las fórmulas $A_1, \dots, A_m$ es verdadera.

La notación

$A_1, \dots, A_m \vDash B$

Significa que la fórmula B es la deducción lógica de las fórmulas$A_1, \dots, A_m$ ($A_1, \dots, A_m$ que conllevan a B lógicamente).

Al recurrir a las tablas de verdad se dirá que la fórmula B es la deducción lógica de las fórmulas $A_1, \dots, A_m$si en las tablas construidas siguiendo la sucesión de átomos $p_{1,\dots}, p_n$, que entrando en $A_1, \dots, A_m$, B, la fórmula B posee el valor "verdadero" en todas las líneas donde, simultáneamente, $A_1, \dots, A_m$toman el valor "verdadero". Dicho de otra manera, la colección de juegos de valores de los átomos para los cuales todas las fórmulas $A_1, \dots, A_m$son verdaderas pertenecen a la colección de juegos de valores de átomos para los cuales la fórmula B es verdadero. La sucesión de átomos $p_{1,\dots}, p_n$, que entran en las fórmulas $A_1, \dots, A_m$, B, puede aparentemente adquirir un orden cualquiera. Ejemplo. $A \rightarrow B,\ A \rightarrow \neg B \vDash \neg A$, Lo que se muestra en la tabla:

$A\ B$	$A \rightarrow B$	$A \rightarrow \neg B$	$\neg A$
V V	V	F	F

V F	F	V	F
F V	V	V	V
F F	V	V	V

A partir de la definición de la deducción lógica se deduce que la tautología conlleva lógicamente de cualquier fórmula de la lógica de afirmaciones, mientras que la contradicción infiere en toda formula.

DEFINICIÓN. Las fórmulas A y B son llamadas *equipolentes (lógicamente equivalentes)* si para una elección cualquiera de valores de verdad de átomos, tomando A y B, las fórmulas A y B toman valores de verdad idénticos.

La notación $A \equiv B$ significa que las fórmulas A y B son equipolentes.

De la definición de la equivalencia lógica de las fórmulas se deriva que las dos tautologías son lógicamente equivalentes igual que las dos contradicciones cualquieras.

La fórmula $A\ es\ equipolente\ a\ B\ sí\ y\ sólo\ sí\ A \vDash B\ y\ B \vDash A$.

TEOREMA 2.1. *Las fórmulas A y B son equipolentes sí y sólo sí la fórmula $A \leftrightarrow B$ es una tautología.*

Se propone al lector elaborar la demostración a modo de ejercicio.

TEOREMA 2.2. (a) $A \vDash B$ Sí y sólo sí $\vDash A \rightarrow B$; (b) $A_1, \ldots, A_m \vDash B$ sí y sólo sí $\vDash A_1 \wedge \ldots \wedge A_m \rightarrow B$.

Demostración. (a) Sea $A \vDash B$. La implicación $A \rightarrow B$ tiene el valor de verdad F si A es "verdadero" con, simultáneamente, B "falso". Ahora bien, en virtud $A \vDash B$planteada, no puede existir tal distribución para los valores de verdad para los átomos que entran en A y B.

Por lo tanto, la formula $A \rightarrow B$ adquiere siempre el valor V, es decir $\vDash A \rightarrow B$.

Plantéese ahora que $\vDash A \rightarrow B$. Se ve que la distribución cualquiera de los valores de verdad de los átomos que entran en A y B para la cual A es verdadera. Como por hipótesis con esta distribución $A \rightarrow B$ es calificada V, B adquiere, conservando esta distribución el valor V. Entonces $A \vDash B$.

(b) A partir de la definición de la conjunción se tiene $A_1, \ldots, A_m \vDash B$ sí y sólo si $A_1 \wedge \ldots \wedge A_m \vDash B$.Asimismo, en virtud de (a),

$A_1, \ldots, A_m \vDash B$ sí y sólo sí $\vDash A_1 \wedge \ldots \wedge A_m \rightarrow B$. □

Ejemplo. $(A \rightarrow B), (B \rightarrow C) \vDash (A \rightarrow C)$, dado que $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$ es una tautología.

TEOREMA 2.3. $A_1, \ldots, A_{m,}\ B \vDash C$ sí y sólo sí $A_1, \ldots, A_m \vDash B \rightarrow C$.

Demostración. Supóngase que $A_1, \ldots, A_{m,}\ B \vDash C$ y demuéstrese entonces que $A_1, \ldots, A_m \vDash B \rightarrow C$. Admítase que existe una distribución de valores de verdad de los átomos que entran en las fórmulas $A_1, \ldots, A_{m,}\ B, C$ por las que las fórmulas $A_1, \ldots, A_m$ tienen por valor V, mientras que la fórmula $B \rightarrow C$ es F. Para esta misma distribución de valores de átomos las fórmulas $A_1, \ldots, A_{m,}\ B$ tomarian simultáneamente el valor V, mientras que la fórmula C sería falsa. Entonces, no existe tal distribución de valores de verdad de los átomos. Por consiguiente, si $A_1, \ldots, A_{m,}\ B \vDash C$, se tiene $A_1, \ldots, A_m \vDash B \rightarrow C$.

Supóngase ahora que $A_1, \ldots, A_m \vDash B \rightarrow C$ y muéstrese que $A_1, \ldots, A_{m,}\ B \vDash C$. Admítase que existe una distribución de valores de verdad de átomos que entran en las fórmulas $A_1, \ldots, A_{m,}\ B, C$ para la que las fórmulas $A_1, \ldots, A_{m,}\ B$ tienen valor V, mientras que las fórmulas C son falsas. Con una distribución idéntica de valores de verdad de átomos de las fórmulas $A_1, \ldots, A_m$toman el valor V y la fórmula $B \rightarrow C$ el valor F, lo que es contradictorio con la hipótesis. Por

consiguiente, no existe tal distribución de valores de verdad para los átomos. Como resultado, A_1, …, $A_m \vDash B \to C$, se tiene A_1, …, $A_m, B \vDash C$. □

COROLARIO 2.4. $A, B \vDash C$ Sí y sólo sí $\vDash A \to (B \to C)$.*Bajo una forma más común:* $A_1, A_2, \ldots, A_m \vDash B$ *sí y sólo sí* $\vDash A_1 \to \big(A_2 \to (\ldots(A_m \to B)\ldots)\big)$.

Para elaborar la demostración es necesario aplicar muchas veces el TEOREMA 2.3.

Se deduce del TEOREMA 2.3 que a las equivalencias tautológicas mencionadas en el TEOREMA 1.3 corresponden las equivalencias lógicas siguientes:

$A \equiv A$;
$A \wedge A \equiv$ A;
$A \vee A \equiv A$;
$A \wedge B \equiv B \wedge A$;
$A \vee B \equiv B \vee A$;
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$;
$A \vee (B \vee C) \equiv (A \vee B) \vee C$;
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$;
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$;
$\neg\neg A \equiv A$;
$(A \leftrightarrow B) \equiv (B \leftrightarrow A)$;
$(A \to B) \equiv (\neg B \to \neg A)$;
$\neg(A \vee B) \equiv \neg A \wedge \neg B$;
$\neg(A \wedge B) \equiv \neg A \vee \neg B$;
$(A \leftrightarrow B) \equiv (\neg A \leftrightarrow \neg B)$;
$A \to (B \to C) \equiv B \to (A \to C)$;
$A \to B \equiv \neg A \vee B$;
$A \to B \equiv \neg(A \wedge \neg B)$;
$A \vee B \equiv \neg A \to B$;
$A \vee B \equiv \neg(\neg A \wedge \neg B)$;
$A \wedge B \equiv \neg(A \to \neg B)$;
$A \wedge B \equiv \neg(\neg A \vee \neg B)$;
$(A \leftrightarrow B) \equiv (A \to B) \wedge (B \to A)$.

Esquemas deductivos. Las Demostraciones de una u otras afirmaciones matemáticas se elaboran en base a reglas determinadas de las que la esencia se traduce por implicaciones tautológicas de la lógica de afirmaciones. Estas dan una imagen esquemática de la marcha de la demostración que por consecuencia se le llaman *esquemas deductivos* o *reglas de Demostraciones* (ver, por ejemplo, más adelante regla de desplazamiento, regla de contraposición, etc.) Dese las reglas correspondientes a las 15 primeras implicaciones tautológicas del TEOREMA 1.3:

$A, A \to B \vDash B$	regla de desplazamiento
$A, B \vDash A \wedge B$	regla de inclusión de la conjunción
$A \wedge B \vDash A$ $A \wedge B \vDash B$	reglas de eliminación de la conjunción

$A \vDash A \vee B$ $B \vDash A \vee B$	reglas de inclusión de la disyunción
$A \vee B, \neg B \vDash A$	regla de eliminación de la disyunción
$A \vDash \neg\neg A$	regla de inclusión de la doble negación
$\neg\neg A \vDash A$	regla de eliminación de la doble negación
$A \to B, B \to A \vDash A \leftrightarrow B$	regla de inclusión de la equivalencia
$A \leftrightarrow B \vDash A \to B$ $A \leftrightarrow B \vDash B \to A$	reglas de eliminación de equivalencias
$A \to B \vDash \neg B \to \neg A$	regla de contraposición
$\neg A \to B, \neg A \to \neg B \vDash A$	regla de demostración a contrario
$A \to B, B \to C \vDash A \to C$	Regla del silogismo
$A \to C, B \to C \vDash A \vee B \to C$	Demostración por análisis de caso

Para notar estas reglas se sigue a menudo las premisas debajo la línea horizontal, mientras que la conclusión se ubica debajo de esta última. En esta notación los esquemas deductivos antes mencionados toman la forma:

$\dfrac{A \to B \quad A}{B}$	Regla de desplazamiento
$\dfrac{A \quad B}{A \wedge B}$	Regla de inclusión de la conjunción
$\dfrac{A \wedge B}{A}$; $\dfrac{A \wedge B}{B}$	Reglas de eliminación de la conjunción
$\dfrac{A}{A \vee B}$; $\dfrac{B}{A \vee B}$	Reglas de inclusión de la disyunción
$\dfrac{A \vee B \quad \neg B}{A}$	Regla de eliminación de la disyunción
$\dfrac{A}{\neg\neg A}$	Regla de inclusión de la doble negación

$\dfrac{\neg\neg A}{A}$ Regla de eliminación de la doble negación

$\dfrac{A \to B \quad B \to A}{A \leftrightarrow B}$ Regla de inclusión de la equivalencia

$\dfrac{A \leftrightarrow B}{A \to B}$; $\dfrac{A \leftrightarrow B}{B \to A}$ Reglas de eliminación de la equivalencia

$\dfrac{A \to B}{\neg B \to \neg A}$ Regla de contraposición

$\dfrac{\neg A \to B \quad \neg A \to \neg B}{A}$ Regla de demostración a contrario

$\dfrac{A \to B \quad B \to C}{A \to C}$ Regla del silogismo

$\dfrac{A \to C \quad B \to C}{A \vee B \to C}$ Demostración por análisis de caso

Demostración indirecta (demostración a contrario). La colección de fórmulasA_1, …, A_m de la lógica de afirmaciones se dice contradictoria si, por una distribución cualquiera de valores de verdad de átomos que las componen, al menos una de las fórmulasA_1, …, A_m adquiere el valor F. Se ve fácilmente que la colección de fórmulasA_1, …, A_m es contradictoria sí y sólo sí la fórmula $A_1 \wedge \ldots \wedge A_m$ es una contradicción, o sea una fórmula siempre falsa.

TEOREMA 2.5. *Si de la colección de fórmulasA_1, …, A_m se desprende lógicamente una contradicción, esta colección de fórmulas entonces es una contradicción.*

Demostración. Plantéese queA_1, …, $A_m \vDash F$, donde F es una fórmula siempre falsa. Entonces, según el TEOREMA 2.3,

$$\vDash A_1 \wedge \ldots \wedge A_m \to F.$$

Conforme a la tabla de verdad de la implicación, se deduce que la formula $A_1 \wedge \ldots \wedge A_m$ es siempre falsa. Por lo tanto, la colección de fórmulas $A_1 \wedge \ldots \wedge A_m$ es una contradicción. □

Las fórmulas siempre falsas (contradicciones) juegan un papel esencial en el método de demostración indirecta llamado igualmente *método de demostración a contrario*. Las Demostraciones de este tipo se basan en el TEOREMA siguiente.

TEOREMA 2.6. Si de la fórmulas A_1, …, A_m,$\neg B$ se desprende lógicamente una contradicción, se tiene entonces A_1, …, $A_m \vDash B$.

Demostración. Plantéese $A_1, \ldots, A_m, \neg B \vDash F,$ donde F es una contradicción. Entonces, según el TEOREMA 2.5, la colección de fórmulas $A_1, \ldots, A_m, \neg B$ es contradictorio. Si por una distribución cualquiera de valores de verdad de átomos que componen las fórmulas $A_1, \ldots, A_m, \neg B$ todas las fórmulas $A_1, \ldots, A_m$ toman el valor V, se obtendrá para la fórmula $\neg B$ el valor F, por tanto, B será calificada V. Entonces, $A_1, \ldots, A_m \vDash B.$ □

Así pues, si es necesario demostrar que cierta afirmación B es lógicamente implicada por premisas dadas, se agrega ¬B a estas premisas y se muestra que de estas premisas se deriva una contradicción (esta toma normalmente la forma $C \wedge \neg C$). Luego de esto, se puede concluir que la afirmación B es la deducción lógica de las premisas de partida. Para $m = 0$ se tiene un caso particular, es decir que faltan las premisas. Si al admitir la verdad de ¬B se llega a la contradicción ($C \wedge \neg C$), es posible. Este razonamiento se apoya en la regla de demostración *a contrario:* $\neg B \rightarrow C, \neg B \rightarrow \neg C \vDash B$.

La demostración por análisis de este caso es muy frecuente: su principio es el siguiente. Supóngase que se trata de demostrar la verdad de la afirmación C. Se construyen las afirmaciones A y B tales como $A \vee B, A \rightarrow C, B \rightarrow C$ sean verdaderas (en respuesta de B se toma a menudo no-A). Luego, en base al esquema deductivo que corresponde se puede afirmar que C es verdadero.

Al apoyarse en la regla del silogismo se puede aplicar la verdad de la afirmación $A \rightarrow B$ si se está en la capacidad de construir la cadena de implicaciones

$$A \rightarrow A_1, \qquad A_1 \rightarrow A_2, \ldots, \qquad A_{n-1} \rightarrow A_n, \quad A_n \rightarrow B,$$

de las que cada una es verdadera.

Ejercicios

1. Demostrar que son basados los esquemas deductivos siguientes:

(a) $\frac{A\to\neg B}{B\to\neg A}$;
(b) $\frac{A,A\leftrightarrow B}{B}$;
(c) $\frac{A\leftrightarrow B}{(B\to C)\to(A\to C)}$;
(d) $\frac{A\leftrightarrow B,B\leftrightarrow C}{A\leftrightarrow C}$;
(e) $\frac{A\leftrightarrow B,C\leftrightarrow D}{A\vee C\leftrightarrow B\vee C}$;
(f) $\frac{A\leftrightarrow B,C\leftrightarrow D}{A\wedge C\leftrightarrow B\wedge D}$;
(g) $\frac{A\to B,C\to D}{A\vee C,B\vee D}$;
(h) $\frac{A\to B,C\to D}{A\wedge C\to B\wedge D}$;
(i) $\frac{A\to B,A\to C}{A\to B\wedge C}$;
(j) $\frac{A\to(B\to C)}{(A\to B)\to(A\to C)}$;
(k) $\frac{A\to C}{A\wedge B\to C}$;
(l) $\frac{A\to(B\to C)}{A\wedge B\to C}$;
(m) $\frac{\neg A}{A\to B}$;
(n) $\frac{A\to B,\neg B}{\neg A}$;
(o) $\frac{(A\wedge\neg B)\to(C\wedge\neg C)}{A\to B}$;
(p) $\frac{A\to A\leftrightarrow B}{B\to(A\to C)}$;
(q) $\frac{A\leftrightarrow(B\to C)}{A\to(\neg C\to\neg B)}$

2. Demostrar que para toda fórmula de la lógica de afirmaciones existe una fórmula de equivalencia lógica construida solamente con la ayuda de una de las siguientes parejas de cópulas:

(a) ¬, → ; (b) ¬,∨; (c) ¬,∧.

3. Demostrar que

(a) $\neg A\vee B, C\to\neg B\vDash A\to\neg C$;
(b) $A\vee B, A\to C, B\to D\ \vDash C\vee D$;
(c) $A\to(B\to C),\neg D\vee A, B\vDash D\to C$;
(d) $A\vee B\to C\wedge D, D\vee E\to F\vDash A\to F$.

§ 3. Predicados

Los medio ofrecidos por la lógica de afirmaciones no son suficientes para analizar numerosos razonamientos matemáticos. Por ejemplo, la lógica de afirmaciones no permite establecer la validez del razonamiento siguiente: “Todo número entero es un número racional; 25 es un número entero, entonces 25 es un número racional”. Ya que en lógica de afirmaciones, las afirmaciones simples a partir de las cuales se construyen las afirmaciones complejas son definidas indivisibles. Estas no se someten al análisis de la estructura en el sentido de relaciones entre los objetos y sus propiedades. Por consiguiente, resulta necesario construir un sistema lógico cuyas reglas permitan estudiar la estructura de afirmaciones consideradas en lógica de afirmaciones como elementales. Este sistema es la lógica de predicados del cual la lógica de afirmaciones constituye una de las partes.

Variables libres. Se utilizan predominantemente en matemáticas de notaciones literales. Ciertas letras implementadas en el texto designan propósitos cualesquiera de cierta clase. Cada una de estas letras conserva generalmente su individualidad, es decir designa siempre el mismo objeto a lo largo de cierta parte del texto. Letras

diferentes se pueden destinar ya sea con un mismo fin, o ya sea con objetos diferentes. Las letras utilizadas se denominan *variables libres*.

Se denomina valores específicos de la variable a los objetos de la clase determinada por la notación de los cuales se utilizó esta variable. Es así que los valores especificados de la variable libre pueden ser afirmaciones. Dicha variable se denomina *proposicional.*

Los valores específicos de la variable libre pueden ser números naturales o enteros. Esta variable libre respectivamente se denomina entonces *natural* o *entera*.

Si los valores especificados de la variable libre son números reales o complejos, entonces la variable es llamada *real* o *compleja.*

Predicados. Sea una proposición

(1) $x + y = 3$

que contiene variables naturales x y y. Esta proposición no es una afirmación ya que no se puede responder a la pregunta: ¿Es falsa o es verdadera? Se le llama *predicado* o *condición* (sobre x y y). Dese otros ejemplos de proposiciones con variables:

(2) x es un número primo;

(3) x es un número par;

(4) x es menor que y;

(5) x es el divisor común de y, z.

Se plantea que los valores específicos de las variables x, yy z son números naturales. Si en las proposiciones (1)-(5) reemplazamos las variables por sus valores específicos, se obtendrá afirmaciones que podrían ser tanto verdaderas como falsas. Por ejemplo,

$0 + 1 = 3$;

2 es un número primo;

3 es un número par;

5 es inferior a 7;

3 es el divisor común de 6 y 12.

DEFINICIÓN. Las proposiciones con variables que resultan afirmaciones luego de la sustitución de variables libres por los valores específicos se denominan *predicados.*

Las proposiciones (1)-(5) se pueden tomar como ejemplos de predicados

Conforme al número de variables libres que componen los predicados que distinguen los predicados con una función de un solo argumento (monódicos), dos argumentos (diádicos), tres argumentos (tríadicos, etc. Los predicados (2) y (3) son monódicos, el (1) y (4) son diádicos y el predicado (5) es tríadico. Las afirmaciones se consideran como predicados en ningún lugar.

Al reemplazar en el predicado un argumento (2) la variable por números naturales nos resultan las afirmaciones:

0 es un número primo;

1 es un número primo;

2 es un número primo;

3 es un número primo, etc.

Algunas de estas afirmaciones son verdaderas. Es así que el predicado dado a un lugar determinado entre los números naturales aquellos que una vez sustituidos por la variable, proporcionan una afirmación verdadera; se puede entonces asimilar a una condición impuesta al valor de la variable libre que compone al predicado. En el ejemplo desarrollado, los números que satisfacen a esta condición son los números primos.

Un predicado con un solo argumento quizás asimilado para una condición impuesta a objetos de la clase dada; un predicado con dos lugares para una condición impuesta a una pareja de objetos de la misma clase, etc.

Los predicados se pueden tratar de maneras diferentes. En álgebra se estudia a menudo los predicados tratados a manera de ecuaciones, desigualdades, así como a manera de sistemas de ecuaciones o de desigualdades. Es así, por ejemplo que la desigualdad $x + x^{-1} > 0$ define un predicado con un argumento, la ecuación $x^2 + y = 0$ un predicado con dos argumentos, mientras que el sistema de ecuaciones $x + y = 0, x - y + z = 0$ define un predicado de tres lugares (siendo x, y, z variables racionales).

Se notaran los predicados por mayúsculas latinas (con índice inferior si es necesario) con indicación entre paréntesis de todas las variables libres que componen el predicado. Por ejemplo, $A(x, y)$ es la notación de un predicado de dos argumentos, $R(x, y, z)$ la de un predicado a tres argumentos y $Q(x_1, \dots, x_{n)}$ la de un predicado a n argumentos.

Posteriormente, se hablará del valor de verdad de un predicado cualquiera en cierto juego de variables libres que le componen entendiendo por esto el valor de verdad de la afirmación obtenida por la sustitución a las variables libres de los valores correspondientes del juego considerado.

La afirmación obtenida llevando en el predicado $R(x_1, \dots, x_{n)}$ el juego de valores específicos $(a_1, \dots, a_{n)}$ en lugar de sus variables se denotará $R(a_1, \dots, a_{n)}$. Si esta afirmación es verdadera (falsa) se dice que el juego de valores $(a_1, \dots, a_{n)}$ satisface (o no satisface) al predicado $R(x_1, \dots, x_{n)}$.

Nótese que es necesario distinguir los predicados que expresan una misma condición, pero compuestas de variables a los valores especificados diferentes. Por ejemplo, el predicado definido por la ecuación $2x - 3 = 0$, donde x es una variable entera, se debe distinguir del predicado definido por la misma ecuación con x considerada como una variable racional. El primer predicado no se califica como verdadero por ninguno de los valores especificados de x, mientras que el segundo es verdadero por el valor especificado de $x = 3/2$. Al definir se debe indicar el dominio de los valores especificados de las variables de este predicado.

Operaciones en los predicados. Los predicados, como las afirmaciones, son calificados V y F y se pueden también someter a operaciones lógicas análogas tal como la de la lógica afirmativa.

Comiéncese por un caso particularmente simple, donde los predicados de un lugar del cual los dominios de valores específicos de las variables coinciden. A partir de dos predicados $P(x)$ y $Q(y)$ se forma un nuevo predicado $P(x) \wedge Q(y)$. Es un predicado de dos variables libres xy y y su valor de verdad para todo un juego (a, b) de los valores específicos de las variables especificadas se define como el valor de verdad de la afirmación $P(a) \wedge P(b)$. De manera análoga se definen los predicados.

$P(x) \vee Q(y)$, $\neg P(x)$, $P\ (x) \rightarrow Q$(y), $P(x) \leftrightarrow Q(y)$.

Debe diferenciarse los predicados: en dos situaciones P $(x) \wedge$ Q (y) del de una situación P $(x) \wedge$Q (x); en la primera se especifica las variables libres x e y independientemente una de la otra, y en la segunda, únicamente la variable libre x .

Se define de manera análoga para los predicados en diversas situaciones (poliácidos) las operaciones de conjunción, disyunción, negación, implicación y equivalencia. Por ejemplo, véase, el caso de los predicados en dos situaciones. Sea P (x, y), Q (y, z) dos predicados de los cuales el dominio de las variables especificas coinciden. $P\ (x, y)$, $\wedge\ \ Q\ (y, z)$ entonces es un predicado en tres situaciones en x, y, z cuyo valor de verdad para toda serie de variables libres especificas (a, b, c) se define como valor de la afirmación $P\ (a, b)\ \wedge\ Q\ (b, c)$. Nótese que al analizar las operaciones referente a los predicados se debe distinguir las variables representadas por letras diferentes de las que se representan por letras idénticas.

Véase algunos ejemplos:

1) $A\,(x)\ \vee\ B\,(x,y)$ predicado en relación a las variables libres x, y;
2) $\neg A\,(y) \wedge \wedge D(z,x)$ predicado en relación a las variables libres x, y, z;
3) $E\,(x,y,z) \rightarrow F\,(z)$ predicado en relación a las variables libres x, y, z.

El predicado $A(x) V\ B\,(x,y)$ adquiere el valor V para la serie de valores (a,b) si al menos una de las afirmaciones $A\,(a)$Y $B\,(a,b)$ es verdadera y, toma el valor F si las dos afirmaciones son falsas. De manera semejante, se puede establecer los valores de verdad de otros predicados por una serie de variables libres.

Deducción lógica. Predicados equivalentes.

Definición. El predicado $A\,(x_1 \ldots, x_{n)}$ se dice *siempre verdadero* si para toda serie de variables específicas de variables libres que componen su valor de verdad es V.

Se puede tomar por ejemplo de predicado siempre verdadero al predicado de tres situaciones definido por la desigualdad $(x+y)^2 + z^2 \geq\geqslant 0$, donde x, y, z son variables racionales.

Sea $A\,(x_1, \ldots, x_m)$ y $B\,(y_1, \ldots, y_n)$ los predicados que poseen dominios idénticos de variables libres específicas.

Definición. El predicado $B\,(y_1, \ldots\ y_n)$ se le llama *deducción lógica del predicado*$A\,(x_1, \ldots, x_m)$si el predicado $A\,(x_1, \ldots, x_m) \longrightarrow B\,(y_1, \ldots, y_n)$ es idénticamente verdadero.

La notación $A\,(x_1, \ldots, x_m) \vDash B\,(y_1, \ldots, y_n)$ significa que el predicado $B\,(y_1\,, \ldots, y_n)$ es la deducción lógica del predicado $A\,(x_1, \ldots \ldots, x_m)$.

Por ejemplo, si x es una variable entera, la notación del predicado $R\,(x)$ « x es un número par», $P\,(x)$ la notación del predicado « x es múltiplo de 4», entonces $R\,(x)$ resulta lógicamente de $P\,(x)$, dicho de otra forma, $P(x) \vDash R\,(x)$.En el caso del predicado $R\,(x)$ no conlleva lógicamente $P\,(x)$.

Tómese dos predicados en n situaciones $A\,(x_1, \ldots, x_n)$y $B(x_1, \ldots, x_n)$ relativo a las mismas variables. El predicado $B(x_1, \ldots, x_n)$ será la deducción lógica del predicado $A\,(x_1, \ldots, x_n)$ si y solo si toda serie de valores de variables $x_1, \ldots, x_n$, que satisfacen al predicado $A\,(x_1, \ldots, x_n)$, igualmente satisface al predicado $B\,(x_1, \ldots, x_n)$.

Se deja al criterio del lector la demostración de esta afirmación.

Definición. El predicado $B\,(z_1, \ldots, z_n)$se denomina *deducción lógica* de predicados $A_1(x_1, \ldots, x_m), \ldots, A_R\,(y_1, \ldots, y_l)$ si el predicado

$A\,(x_1, \ldots, x_m) \wedge \ldots \wedge A_R(y_1, \ldots, y_l) \rightarrow B\,(z_1, \ldots, z_n)$

es idénticamente verdadero. (Supóngase en el caso que todas las variables libres de los predicados considerados posean los mismos valores específicos).

Ejemplo. Sea $P\,(x)$ el predicado « x es un número par», $Q\,(x)$ el predicado « x es múltiplo de 3», $R(x)$ el predicado « x es múltiplo de 6». Entonces, $P\,(x), Q\,(x) \vDash R\,(x)$.

Definición. Los predicados $A\,(x_1, \ldots, x_m)$ y $B\,(y_1, \ldots, y_n)$ se denomina *equivalentes (lógicamente equivalentes) si* el predicado $A\,(x_1, \ldots, x_m) \leftrightarrow B\,(y_1, \ldots, y_n)$ es idénticamente verdadero. La notación $A\,(x_1, \ldots, x_m) \equiv B\,(y_1, \ldots, y_n)$ significa que los predicados $A\,(x_1, \ldots, x_m)$ y $B\,(y_1, \ldots, y_n)$ son equivalentes.

Se ve fácilmente que los predicados $A\,(x_1, \ldots, x_m)$ y $B\,(y_1, \ldots, y_n)$ son equivalentes si y sólo si

$A\,(x_1, \ldots, x_m) \vDash B\,(y_1, \ldots, y_n)$ Y

$B\,(y_1, \ldots, y_n) \vDash A\,(x_1, \ldots, x_m)$.

Es fácil demostrar que los predicados $A\,(x_1, \ldots, x_m)$ y $B\,(y_1, \ldots, y_n)$ son equivalentes si y solo si sus valores de verdad coinciden para toda serie de valores específicos de variables $x_1, \ldots, x_n$. se puede dar como ejemplo de predicados equivalentes los predicados definidos por las ecuaciones $x^3 - y^3 = 0$ y $2\,(x-y)(x^2+xy+y^2) = 0$, donde x, y son variables racionales.

Definición. El predicado $A\ (x_1, \dots, x_n)$ se denomina idénticamente falso si su valor de verdad es calificado F para toda serie de valores específicos de variables libres en las que aparecen.

Por ejemplo, es idénticamente falso el predicado $x + 1 = x$, donde x es una variable entera.

DEFINICIÓN. El predicado $A\ (x_{1,\dots,}x_n)$ se denomina *realizable* si al menos hay una serie de valores de variables libres en la que aparecen para la cual su valor de verdad es V.

Por ejemplo, son realizables los predicados tales como « x es un número primo», « x es divisible con y», « $x^2 - 5x + 6 = 0$» ,donde x es una variable entera.

Partiendo de las definiciones antes mencionadas resulta que un predicado idénticamente verdadero se deduce lógicamente de todo predicado, mientras que un predicado idénticamente falso resulta lógicamente todo predicado. Todo predicado es ya sea idénticamente verdadero, realizable o idénticamente falso.

Ejercicios:

1. Dar ejemplos de predicados $P(x, y, z)$ y $R\ (x, y, z)$, donde x, y, z son variables naturales, de la cual una es deducción lógica de la otra.
2. Dar ejemplos de predicados en una, dos y tres situaciones que sean idénticamente falso, idénticamente verdadera y realizable (pero no idénticamente verdadera).
3. Construir los predicados $A\ (x)$y $B(x)$donde x es una variable entera, de manera que
   (a) Los predicados $A\ (x)$y $B(x)$ sean no idénticamente verdadero, mientras que $A(x) \vee B\ (x)$ Lo sea;
   (b) $A(x)$ y $B\ (x)$ sean predicados realizables, y $A(x) \wedge B\ (x)$un predicado no realizable.

§ 4. Cuantificadores.

Examínense nuevas operaciones que aplicadas a los predicados o bien a las afirmaciones proporcionen, una vez realizadas, predicados o afirmaciones. Estas operaciones constituyen expresiones de universalidad o existencia.

Cuantificador universal. Sea $A\ (x)$ el predicado de una variable libre x. Por la expresión $\forall\ xA\ (x)$se designará la afirmación que será verdadera si $A\ (x)$ adquiere el valor de Vpara todos los valores específicos de la variable x, es decir si el predicado $A\ (x)$ es idénticamente verdadero, y el valor F el caso contrario. La afirmación $\forall\ xA\ (x)$ es así independiente de x. El símbolo $\forall x$ situado a la izquierda del predicado $A\ (x)$ se denomina *cuantificador universal* que sigue la variable(x). Si, al contrario, A es una afirmación, $\forall\ xA$ entonces es una afirmación verdadera si y solo si A es verdadero.

Ahora pásese a un predicado con múltiples variables libres, por ejemplo el predicado de tres variables $A(x, y, z)$. Este predicado, después de la sustitución arbitraria de todas las variables libres, salvo x, por sus valores b y c, constituye un predicado relativo solamente a la variable x, y la expresión

$$\forall xA\ (x, b, c)$$

es una afirmación. El predicado $\forall xA\ (x, y, z)$ se transforma en una afirmación después de la especificación de todas las variables libres que lo componen, salvo x , y, que parte, no depende de x. $\forall xA\ (x, y, z)$,y de esta manera la función de todas las variables libres que la forman $A\ (x, y, z)$, salvo x, así pues un predicado en dos situaciones referente a yy z. Este predicado para la serie dada de vectores de variables libres b, c se califica V si y solo si el predicado $A\ (x, b, c)$que solo depende de una sola variable libre x es idénticamente verdadera. El símbolo $\forall x$ se lee « para cualquier x « o « para toda x», mientras que la notación $\forall xA\ (x, y, z)$ se lee « cualquier x se tiene $A\ (x, y, z)$» o, de manera más concisa, « para toda $x\ A\ (x, y, z)$ ».

La variable x cuyo predicado $\forall x A\ (x, y, z)$ no depende, denomina *variable ligada* (para diferenciarla de las variables y, z que son variables libres).

Cuantificador existencial. Se utiliza para el cuantificador existencial el símbolo $\exists x$ ubicado a la izquierda del predicado o de la afirmación. Sea $A(x)$ un predicado de variable libre (x). Por la expresión $\exists x\ a\ (x)$ se interpretará la afirmación como verdadera si y solo si $A\ (x)$ se califica V al menos para uno de los valores específicos de la variable (x), (el predicado $A(x)$ es realizable), y falso, en el caso contrario. Si, en cambio, A es una afirmación, $\exists x\ A$ también es una afirmación que es verdadera si y solo si A es verdadero.

Supóngase que $A\ (x, y, z)$ es un predicado en tres situaciones. Si en el predicado en todas las variables libres, salvo x, sustituye sus valores, por ejemplo,b, c, se obtendrá entonces el predicado $A\ (x, b, c)$ que no depende solo de una variable x, y la expresión

$\exists x A\ (x, b, c)$

será una afirmación. Entonces expresión $\exists x A\ (x, y, z)$ es un predicado que se modifica en una afirmación después de la especificación de todas las variables libres, salvo x, y, por consiguiente, no depende de x. Así, la expresión $\exists x A\ (x, y, z)$ es un predicado que solo es función de y y de z, dado que la aplicación de un cuantificador al predicado en tres situaciones le hace pasar a un predicado en dos situaciones. La variable x cuyo predicado $\exists x A\ (x, y, z)$ no depende de esta y se le denomina como *variable ligada*.

El predicado $\exists x A\ (x, y, z)$toma el valor V con la serie dada de valores específicos b, c si y solo si el predicado en una situación $A(x, b, c)$ es realizable.

El símbolo $\exists x$ se denomina cuantificador existencial que sigue la variable x se lee: « existe un x». La expresión $\exists x A\ (x, y, z)$ se lee: « $A\ (x, y, z)$ existe al menos para un x» o bien « existe un x tal que $A(x, y, z)$».

Se aplica los cuantificadores de manera absolutamente análoga en predicados en un número de variables más grande. La asociación de un cuantificador en un predicado en n situación (para $n > 0$) modifica el ultimo predicado en $(n - 1)$ situaciones.

En un mismo predicado es posible asociar repetidas veces los cuantificadores. Por ejemplo, después de haberse asociado al predicado $A\ (x, y)$ el cuantificador existencial seguida la variable x se obtiene el predicado en una situación $\exists x A\ (x, y)$ al cual se puede asociar de nuevo al cuantificador existencial o bien al cuantificador universal seguida la variable y. Finalmente se obtiene la afirmación

$\exists y(\exists x A\ (x, y))$ O bien $\forall y\ \big(\exists x A\ (x, y)\big)$.

Generalmente se elimina los paréntesis y se obtiene las expresiones

$\exists y \exists x A\ (x, y)$ O bien $\forall y\ \exists x A\ (x, y)$.

Nótese que los cuantificadores idénticos se pueden transferir, obteniendo afirmaciones equivalentes, dicho de otra manera, equivalentes verdaderos:
$\forall x \forall y(x, y) \leftrightarrow \forall y \forall x A(x, y)$;
$\exists x \exists y A\ (x, y) \leftrightarrow \exists y \exists x A(x, y)$;
en efecto, las afirmaciones $\forall x \forall y(x, y)$y $\forall y \forall x A(x, y)$ las dos son verdaderas si y solo si el predicado $A(x, y)$ es idénticamente verdadero. Las afirmaciones $\exists x \exists y A\ (x, y)$ y $\exists y \exists x A(x, y)$ si y solo si las dos son verdaderas si $A(x, y)$ es un

predicado realizable. Sin embargo, si se asocia al predicado sucesivamente a cuantificadores diferentes, el orden de dicha sucesión es esencial. Por ejemplo, las afirmaciones $\forall y \exists x A\,(x, y)$ y $\exists x \exists y A(x, y)$ propiamente no se expresan equivalentes, es decir que ellas pueden tener valores de verdad diferentes.

La asociación en un predicado de uno o más cuantificadores (universal, existencial) se denomina *cuantificación.*

Véase un ejemplo de cómo se aplica los cuantificadores. Sea $x + y > 0$ un predicado en dos situaciones donde x y y son variables enteras. El predicado expresa la positividad de una suma de dos números enteros y constituye una afirmación cada vez que las variables x y y son especificas. Si se asocia a este predicado un cuantificador existencial que sigue de la variable y se modifica en un predicado en una situación

$\exists y(x + y > 0).$

Cuando se define la variable x del predicado, este último se convierte en una afirmación. El predicado $\exists y(x + y > 0)$es verdadero cuando los valores de la variable x proporcionan un entero y que forma al sumarse con $x$un número positivo. Se demuestra fácilmente que el predicado es idénticamente verdadero, y si se asocia a este último cuantificador universal en x, se obtiene entonces una afirmación

$$\forall x \exists y(x + y > 0),$$

que requiere que para todo número entero x existe un cierto número entero y que restituye su suma positiva. Esta afirmación se diferencia de la siguiente afirmación

$$\exists y \forall x(x + y > 0),$$

que afirma que existe un número entero en el cual la suma con cualquier número entero es positivo. Esta última afirmación es falsa.

Notación de las afirmaciones en el lenguaje de la lógica de los predicados. Examínese cuatro tipos principales de afirmaciones que se encuentran frecuentemente en matemáticas. En la notación simbólica de las afirmaciones (el lenguaje de la lógica de los predicados) se emplea los cuantificadores.

Sea $A(x)$la notación del predicado « x es un número impar» y $B\,(x)$ la notación del predicado « x es un número primo», donde x es una variable entera.

1. La afirmación « todo número impar es un número primo» puede ser enunciado de la manera siguiente: « para toda x, si x es impar, x es un número primo». Entonces llega a ser evidente que en el lenguaje de predicados esta afirmación se denotará así:

$$\forall x(A(x) \to B(x)).$$

2. La afirmación « ningún número impar constituye un número primo « o « para toda x, si x es impar, x no es primo « se anotará simbólicamente así:

$$\forall x\big(A(x) \to \neg B(x)\big).$$

Obsérvese que en nuestro razonamiento el valor de verdad de la afirmación no juega ningún papel.

3. El siguiente tipo de afirmación es de la forma « algunos números impares son primos ». Quiere decir que existe un x que es simultáneamente impar y primo. También la afirmación del tercer tipo se anotará en el lenguaje de predicados bajo la forma

$\exists x\big(A(x) \wedge B(x)\big).$

Esta última notación no equivale a la notación

$\exists x\big(A(x) \to B(x)\big)$,

cuyo sentido es diferente al de la afirmación del principio.

4. El cuarto tipo de afirmación es de la forma: «algunos números impares no son primos». Esta afirmación se denota así:
   $\exists x\big(A(x) \wedge \neg\, B\,(x)\big)$.

   Los ejemplos analizados muestran que cada afirmación que pertenece a uno de cuatro tipos principales se presta a una notación simbólica.

   En la sucesión para enunciar la afirmación «existe un x positivo tal que $A(x)$», en lugar de la notación simbólica

   $$\exists x\,(x > 0 \wedge A(x))),$$

   Se utilizará una anotación más concisa $(\exists x > 0)\ A\ (x)$. De manera semejante para la afirmación « para todo x positivo se tiene $A\ (x)$ » en lugar de
   $\forall x\ (x > 0 \to A(x))$
   se empleará la notación $(\forall x > 0)A\ (x)$.

Ejercicios

1. Escribir en el lenguaje de predicados las siguientes afirmaciones:

(a) Algunos números reales son números racionales.
(b) Ningún número primo no es un cuadrado exacto.
(c) Algunos números pares no se dividen por 8.
(d) Todo múltiplo de 6 se divide por 3.

2. $P(x)$ representa «x es un número primo», $Q\ (x)$ «x es un número par», $R\ (x)$ «x es un número entero», $D\ (x, y)$ «x se divide con y». Formular utilizando palabras en las siguientes afirmaciones escritas en el lenguaje de predicados. Diferenciar las que son verdaderas de las que son falsas:
   (a) $\forall x P\big(x \to \neg Q(x)\big)$;
   (b) $\forall x\ \Big(\neg P\ (x) \to \forall\, y\big(P(y) \to \neg D(x, y)\big)\Big)$;
   (c) $\forall x\ \Big(Q(x) \to \forall y\big(D(x, y) \to Q(y)\big)\Big)$;
   (d) $\forall x \exists y\big(R(x) \wedge R(y) \to D(x, y)\big)$;
   (e) $\forall y \forall x\big(R(x) \wedge R(y) \to D(x, y)\big)$;
   (f) $\exists x\ \forall y\ \big(R\ (x) \wedge R\ (y) \to D(x, y)\big)$.

3. Al utilizar símbolos lógicos al escribir las siguientes afirmaciones:

(a) Los números 5 y 12 no tienen divisores comunes diferentes de +1 y -1.
(b) El número natural divisible por seis es igualmente divisible por 2 y por 3-
(c) Para todo número entero x existe un número entero y que verifica sea $x = 2y$, Sea $x = 2y + 1$.
(d) Todo número natural tiene un número natural superior a él.
(e) Existe un número natural mínimo.
(f) El sistema de ecuaciones $x + y = 0,\ x + y = 1$ no admite solución (sistema incompatible).
(g) No existe número racional x tal que $x^2 - 2 = 0$.

(h) Para todo número entero x y z existe un número entero y tal que $x + y = z$.

(i) Para dos números racionales x y y existe un número racional z tal que $x < z$ y $z < y$.

4. Buscar si para todos los predicados $P\ (x, y), Q\ (x), R(x)$ se obtiene los equivalentes siguientes: sino, dar ejemplos de predicados que lo confirmen:

(a) $\forall x \exists y\ P\ (x, y) \equiv \exists y \forall x P(x, y)$;

(b) $\forall x \forall y\ P\ (x, y) \equiv \forall y \forall x P\ (x, y)$;

(c) $\forall x\ \big(R(x) \vee Q(x)\big) \equiv \forall x R(x) \vee \forall x Q(x)$;

(d) $\exists x\ \big(R\ (x) \wedge Q(x)\big) \equiv \exists x\ \big(R\ (x) \wedge \exists Q(x)\big)$;

(e) $\forall x \forall y\ \big(R(x) \vee Q(y)\big) \equiv \forall x\ R(x) \vee \forall x\ Q(x)$;

(f) $\forall x Q\ (x) \to \exists x R(x) \equiv \exists x\big(Q(x) \to R(x)\big)$;

(g) $\exists x\ R(x) \vee \forall x Q(x) \equiv \exists x\big(R(x) \to Q(x)\big)$;

(h) $\forall x\ \big(R(x) \to Q(x)\big) \equiv \forall x R(x) \to \forall x Q(x)$.

§ 5. Fórmulas de predicados. Leyes lógicas.

Fórmulas elementales. Supóngase que se dispone de una lista de variables:

$$x, y, z, u, w, \dots, x_1, y_1, z_1, u_1, w_1, \dots,$$

denominados generalmente *objetos variables*, porque se sustituyen nombres de objetos determinados.

$a, b, c, a_1, b_1, c_1, \dots$

Además se admite que para cada n natural se posee un cierto conjunto de expresiones.

$P\ (x_1, x_2, \dots, x_n), \qquad Q(x, y, \dots, t), \qquad R(y_1, \dots, y_n), \dots,$

Denominados *símbolos predicativosn*-areos (en n situaciones). Por ejemplo, $P\ (x), Q\ (y)$ son símbolos predicativos simples (en una situación), $P\ (x, y),\ Q(x_1, x_2)$ binarios (en dos situaciones), $P\ (x, y, z),\ Q(x_1, x_2, x_3)$ ternarios (en tres situaciones), $A, B, \dots P, Q$ nularios (en ninguna situación). Partiendo de esta colección de símbolos predicativos se forman expresiones que se denominarán fórmulas elementales o predicados atómicos de la lógica (átomos de la lógica de predicados).

DEFINICIÓN. Se le denomina *fórmula elemental* a la expresión obtenida por sustitución en el símbolo predicativo a las variables $(x, y, \dots)$ que la componen algunos objetos variables no obligatoriamente diferentes.

Por ejemplo, partiendo del símbolo predicativo simple $P(x)$, resultan las fórmulas elementales (átomos) $P(x), P(y), P(u)$,etc.; partiendo del símbolo predicativo binario $Q(x, y)$, se obtienen las fórmulas elementales $Q(x, y), Q(y, z), Q(u, v), Q(x, x), etc$. Partiendo del símbolo predicativo $R\ (x, y, z)$, se obtienen las fórmulas elementales $R\ (x, y, z),\ R(y, z, x),\ R\ (x, x, x), R(x, y, x)$, etc. Los símbolos predicativos iniciados en ninguna situación también se incluyen en la colección de las fórmulas elementales. Las fórmulas elementales constituyen una colección más vasta que la colección de salida de los símbolos predicativos, dado que los objetos variables que entran en las fórmulas elementales no son obligatoriamente diferentes.

Fórmulas predicativas. Las *fórmulas predicativas* (fórmulas de la lógica de predicados) se incorporan de la manera siguiente:

(a) toda fórmula elemental es una fórmula predicativa,

(b) si $\boldsymbol{A}$ Y $\boldsymbol{B}$ son fórmulas predicativas $(\neg \boldsymbol{A})$, $(\boldsymbol{A} \wedge \boldsymbol{B}),(\boldsymbol{A} \vee \boldsymbol{B}), (\boldsymbol{A} \rightarrow \boldsymbol{B})$Y $(\boldsymbol{A} \leftrightarrow \boldsymbol{B})$ igualmente son fórmulas predicativas. Si $\boldsymbol{A}$ es una formula predicativa y x un objeto variable, $(\forall \boldsymbol{x}\boldsymbol{A})$ Y $(\exists \boldsymbol{x}\boldsymbol{A})$ son también fórmulas predicativas,

(c) una expresión solo es una fórmula predicativa si ella es una fórmula elemental o si se construye con fórmulas elementales por aplicación sucesiva de reglas (a),(b).

Las fórmulas predicativas que no son elementales se les denomina *fórmulas predicativas compuestas.*

Para la notación de fórmulas de la lógica de predicados se valdrá de letras mayúsculas en negrita: $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \dots, \boldsymbol{R}, \boldsymbol{P}, \boldsymbol{Q}$,etc.

En las fórmulas $(\forall \boldsymbol{x}\boldsymbol{A})$ y$(\exists \boldsymbol{x}\boldsymbol{A})$ la fórmula $\boldsymbol{A}$ se denomina *dominio de acción de cuantificadores*$\forall x$ y $\exists x$ respectivamente.

Generalmente es apropiado eliminar los paréntesis. Además, se plantea que los cuantificadores tienen una fuerza comunicativa superior que las otras operaciones. Por consiguiente la fórmula $\big(\forall \boldsymbol{x}\boldsymbol{P}(\boldsymbol{x})\big) \rightarrow \boldsymbol{R}(\boldsymbol{x}, \boldsymbol{y})$ puede escribirse $\forall \boldsymbol{x}\boldsymbol{P}(\boldsymbol{x}) \rightarrow \boldsymbol{R}(\boldsymbol{x}, \boldsymbol{y})$.

DEFINICIÓN. La fórmula predicativa se denomina *universal* si después sustituye fórmulas elementales que la compone por predicados cualesquiera, obteniéndose un predicado siempre verdadero.

DEFINICIÓN. Las fórmulas predicativas se denominan *equivalentes* si después sustituye las fórmulas elementales que las componen de fórmulas predicativas cualesquiera, obteniéndose predicados equivalentes. La equivalencia de las fórmulas $\boldsymbol{A}$ Y $\boldsymbol{B}$ se denotará así: $\boldsymbol{A} \equiv \boldsymbol{B}$.

Se demuestra fácilmente que la fórmula predicativa $\boldsymbol{A} \leftrightarrow \boldsymbol{B}$ es universal si y solo si $\boldsymbol{A}$ y$\boldsymbol{B}$ son fórmulas predicativas equivalentes.

Una serie de equivalencias de la lógica de predicados se puede obtener de equivalencias de la lógica de afirmaciones. Por ejemplo, los equivalentes de la lógica de afirmaciones.

$A \wedge B \equiv B \wedge A$;
$\neg\neg A \equiv A$;
$\neg(A \vee B) \equiv \neg A \wedge \neg B$;
$\neg(A \wedge B) \equiv \neg A \vee \neg B$
3-01762

Corresponden equivalentes de la lógica de predicados.

$\boldsymbol{A} \wedge \boldsymbol{B} \equiv \boldsymbol{B} \wedge \boldsymbol{A}$;
$\neg\neg \boldsymbol{A} \equiv \boldsymbol{A}$;
$\neg(\boldsymbol{A} \vee \boldsymbol{B}) \equiv \neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$;
$\neg (\boldsymbol{A} \wedge \boldsymbol{B}) \equiv \neg \boldsymbol{A} \vee \neg \boldsymbol{B}$.

De manera análoga las fórmulas idénticamente verdaderas de la lógica de afirmaciones constituyen el origen donde son extraídas las fórmulas universales de la lógica de predicados. Por ejemplo, en la tautología $A \vee \neg A$ corresponde la fórmula universal de la lógica de predicados $\boldsymbol{A} \vee \neg \boldsymbol{A}$**.** En efecto, al llevar predicados cualquieras en toda fórmula $\boldsymbol{A}$ precisando el lugar de los símbolos predicativos que la componen, obteniéndose un cierto predicado $P\ (x_1, \dots, x_n)$. La fórmula $\boldsymbol{A} \vee \neg \boldsymbol{A}$se transforma en el caso de predicado $P\ (x_1, \dots, x_n) \vee \neg P\ (x_1, \dots, x_n)$ que adquiere el valor V para todos los valores específicos de variables (en virtud de la ley del tercer excluido de la lógica de afirmaciones).

Así mismo al razonar, se está en la capacidad de validar las otras fórmulas universales y equivalentes de la lógica de predicados transferidos de la lógica de afirmaciones.

Además las fórmulas universales y las equivalencias de la lógica de predicados obtenidos de esta manera, existen fórmulas universales y de equivalencias específicas correspondientes al uso de los cuantificadores. Se analizará algunas.

Leyes de la lógica de predicados. Se estudia una serie de equivalencias que juegan un gran papel en la lógica de predicados. No se plantearán demostraciones rigurosas.

La equivalencia

(1) $\neg\left(\forall x A\,(x)\right) \equiv\ \exists x\left(\neg\, A\,(x)\right)$

corresponde a la interpretación general de cuantificadores. Las afirmaciones «es falso que todo objeto x satisface a la condición $A\,(x)$ » y « existe un objeto x que no satisface a la condición $A\,(x)$» tienen el mismo significado que expresa la equivalencia (1).

La equivalencia

(2) $\neg\,(\exists x A\,(x))\ \equiv\ \forall x\,(\neg\, A\,(x))$

corresponde a la identificación general de las afirmaciones «es falso que existe un objeto x que satisface a la condición $A\,(x)$» y «ningún objeto x satisface a la condición $A\,(x)$ ».

Al aplicar la negación a los dos elementos de (1) y (2) y, teniendo en cuenta la ley de la doble negación, resulta a un en dos equivalencias

(3) $\forall x A\,(x)\ \equiv \neg\left(\exists x \neg\, A\,(x)\right)$;

(4) $\exists x A\,(x) \equiv \neg\left(A x \neg\, A\,(x)\right)$;

estás últimas muestran que el cuantificador existencial puede expresarse al medio del cuantificador universal y recíprocamente.

Las dos equivalencias siguientes traducen las propiedades de distributivas del cuantificador universal relativamente a la conjunción y del cuantificador existencial relativamente a la disyunción:

(5) $\exists x A\,(x)\ \vee\ \exists x B\,(x)\ \equiv\ \exists x\left(A\,(x)\ \vee B\,(x)\right)$;

(6) $\forall x A\,(x) \wedge\ \forall x\left(A\,(x)\ \wedge B\,(x)\right)$.

A decir verdad estas equivalencias se asocian a los importantes razonamientos siguientes. El primer elemento de (5) adquiere el valor V si y solo si o bien $A\,(x)$, o bien $B(x)$ se califican$V$ al menos por un valor específico de x, es decir cuando al menos uno de los predicados $A(x)\ y\ B\,(x)$ es válido. Sin embargo, es precisamente en este caso y solo en el caso que sea válido el predicado $A\,(x) \vee B\,(x)$, es decir será verdadera la afirmación $\exists x(\,A\,(x) \vee B\,(x))$. Para la equivalencia pueden llevarse a cabo razonamientos semejantes (6).

El cuantificador existencial no es relativamente distributivo a la conjunción, es decir que las fórmulas $\exists x(\,A\,(x) \wedge B\,(x))$ Y $\exists x A\,(x) \wedge \exists x B\,(x))$ no son equivalentes. No es difícil encontrar un ejemplo de dos predicados realizables cuya conjunción sea no realizable. Para tales predicados la primera fórmula se califica F, y la segunda, V. Las fórmulas $\forall x(\,A\,(x) \vee B\,(x))$ y $\forall x A\,(x) \vee \forall x B\,(x)$ igualmente son no equivalentes, dicho de otra manera, el cuantificador universal no es relativamente distributivo en la disyunción.

A cada equivalencia de la lógica de predicados corresponde una fórmula universal. Por ejemplo: serán universales las fórmulas siguientes (se les domina con frecuencia *leyes lógicas)*:

(1) $\neg\left(\forall \boldsymbol{x A}\,(\boldsymbol{x})\right) \leftrightarrow\ \exists \boldsymbol{x}\left(\neg\, \boldsymbol{A}(\boldsymbol{x})\right)$;

(2) $\neg\left(\exists \boldsymbol{x A}\,(\boldsymbol{x})\right) \leftrightarrow\ \forall \boldsymbol{x}\left(\neg\, \boldsymbol{A}(\boldsymbol{x})\right)$;

(3) $\forall \boldsymbol{x A}\,(\boldsymbol{x}) \leftrightarrow\ \neg(\exists \boldsymbol{x} \neg\, \boldsymbol{A}(\boldsymbol{x}))$;

(4) $\exists x A\,(x) \leftrightarrow\ \neg\,(\forall x \neg\, A(x))$;

(5) $\exists x A\,(x)\ \vee\ \exists x B(x) \leftrightarrow\ \exists x\,(A\,(x) \vee B(x))$;

(6) $\forall x A\,(x)\ \wedge \forall x B(x) \leftrightarrow\ \forall x\,(A\,(x) \wedge B(x))$.

Existe en la lógica de afirmaciones un método general que permite en un número finito de operaciones para despejar para cualquier fórmula proposicional si esta última es idénticamente verdadera (método de tabla de verdad). En lógica de predicados no se conoce de método tan general que permita en un número finito de operaciones a dilucidar para cualquier fórmula predicativa si esta última es universal o no. Para algunos tipos de fórmulas se elaboró métodos semejantes.

Ejercicios

1. Buscar si las fórmulas siguientes son universales (sino confirmarla por ejemplos):

(a) $\exists x P \rightarrow \forall x P\,(x)$;

(b) $\forall x P\,(x) \rightarrow p\,(y)$;

(c) $P(y) \rightarrow \forall x P\,(x)$;

(d) $\exists x Q\,(x)\ \rightarrow Q\,(y)$;

(e) $\forall x \exists y Q\,(x, y) \rightarrow\ \exists y \forall x Q\,(x, y)$;

(f) $\forall x \forall y \forall z\,(P\,(x, y) \wedge P\,(y, z) \rightarrow P(x, z))$;

(g) $\forall x P\,(x) \vee \forall x Q\,(x) \leftrightarrow\ \exists x\,(P(x) \wedge Q(x))$;

(h) $\forall x\,(P\,(x) \leftrightarrow Q(x)) \rightarrow \exists(x P\,(x) \leftrightarrow \exists x Q\,(x))$;

(i) $\exists x P(x) \wedge \exists x Q\,(x) \rightarrow \exists x\,(P(x) \wedge Q(x))$;

(j) $\forall x\,(P(x) \vee Q\,(x)) \rightarrow \forall x P(x) \vee\ \forall x Q\,(x)$.

2. Mostrar la Pertinencia de universalidad de las fórmulas siguientes:

(a) $\forall x P\,(x) \vee\ \forall x Q\,(x) \rightarrow\ \forall x\,(P\,(x) \vee Q\,(x))$;

(b) $\exists x(P\,(x) \wedge Q\,(x)) \rightarrow\ \exists x P\,(x) \wedge \exists x Q\,(x)$;

(c) $\forall x\,(P\,(x) \rightarrow\ Q\,(x))\ \rightarrow (\forall x P\,(x) \rightarrow \forall x Q\,(x))$;

(d) $\forall x\,(P\,(x) \leftrightarrow Q(x)) \rightarrow (\forall x P\,(x)\ \leftrightarrow \forall x Q\,(x))$;

(e) $\forall x\,(P\,(x) \rightarrow Q(x)) \rightarrow (\exists x P\,(x)\ \rightarrow \exists x Q\,(x))$;

(f) $\forall x Q\,(x) \rightarrow \exists x Q\,(x)$;

(g) $\forall x P\,(x)\ \rightarrow P(y)$;

(h) $Q\,(y) \rightarrow \exists x Q\,(x)$;

(i) $\neg\neg\, \forall x P\,(x, y) \rightarrow \forall x P\,(x, y)$;

(j) $\forall x \forall y P\,(x, y) \leftrightarrow \forall y \forall x P(x, y)$;

(k) $\exists x\, \exists y R\,(x, y) \leftrightarrow \exists y\, \exists x R\,(x, y)$;

(l) $\exists x P\,(x)\ \wedge \exists x Q\,(x) \leftrightarrow\ \exists x\, \exists y\,(P\,(x)\ \wedge Q\,(y))$;

(m) $\forall x R\,(x)\ \vee\ \forall x Q\,(x) \leftrightarrow \forall x\, \forall y\,(P\,(x)\ \vee Q(y))$;

(n) $\forall x Q\,(x, z) \leftrightarrow \forall y Q\,(y, z)$;

(o) $\exists x P\,(x, z) \leftrightarrow\ \exists y P\,(y, z)$;

(p) $\forall x\, \neg\, P\,(x) \vee\ \forall x Q\,(x) \leftrightarrow\ \exists x P\,(x) \rightarrow \forall x Q\,(x)$;

(q) $\exists x\,(P\,(x) \rightarrow Q\,(x)) \leftrightarrow \forall x P\,(x) \rightarrow \exists x Q(x)$.

(r) $\exists x(P(x) \rightarrow Q(x)) \leftrightarrow \forall z P(x) \rightarrow \exists x Q(x)$.

CAPITULO II
CONJUNTOS Y RELACIONES

§ 1. CONJUNTOS

Noción de conjunto. La noción de conjunto es una de las más importantes en matemáticas. Se le denomina *conjunto* a una colección de objetos (artículos materiales o nociones abstractas) consideradas como un todo. Por ejemplo, se puede hablar de conjunto de todos los números naturales, el conjunto de letras de una página, el conjunto de raíces de una ecuación dada, etc. Los objetos que componen un conjunto se denominan *elementos*. La noción de conjunto se considera como intuitiva, primaria, es decir que no se puede reducir a otras nociones.

Las afirmaciones «El objeto a es un elemento del conjunto A», «El objeto a pertenece al conjunto A» cuyo significado es el mismo pueden escribirse de manera compacta bajo la forma $a \in A$.

Si el elemento a no pertenece al conjunto A, se denota $a \notin A$.

El símbolo ∈ se denomina *signo de pertenencia.*

DEFINICIÓN. Dos conjuntos A y B se denominan i*guales* y se denota $A = B$ si A y B contienen los mismos elementos.

Así, los *conjuntos*A y B son *iguales* si para todo x $x \in A$ si y solo si $x \in B$. Por consiguiente, la demostración de igualdad de dos conjuntos dados A y B generalmente corresponden a la demostración de dos afirmaciones: 1) Para toda x si $x \in A, x \in B$; 2) para toda x si $x \in B, x \in A$.

Frecuentemente se representa un conjunto por sus elementos puestos entre llaves. Es así, por ejemplo, que el conjunto compuesto de elementos a, b, c, se denota $\{a, b, c\}$. El conjunto compuesto de elementos $a_1, a_2, \dots, a_n$ se representa por $\{a_1, a_2, \dots, a_n\}$.

Los conjuntos $\{1, 2, 3\}$ y $\{3, 1, 2, 1\}$ son iguales, porque cada elemento del primer conjunto pertenece al segundo conjunto y recíprocamente. Los dos están compuestos de tres elementos. General mente se utiliza la notación $\{1, 2, 3\}$.

Un conjunto puede estar compuesto de un solo elemento. Debe diferenciarse el elemento a del conjunto $\{a\}$ solo contiene un único elemento a, ya que se admite la existencia de conjuntos cuyos elementos constituyen ellos mismos conjuntos. Por ejemplo, el conjunto $a = \{2, 1\}$ se compone de dos elementos 2 y 1; el conjunto $\{a\}$ tiene un único elemento a que de su lado posee dos elementos.

Subconjuntos.

DEFINICIÓN. El conjunto A se denomina *subconjunto* del conjunto B si cada elemento del conjunto A pertenece al conjunto B.

Si A es un subconjunto del conjunto B, se dice igualmente que A se contiene en B y se denota $A \subset B$. El símbolo ⊂ se denomina *símbolo de inclusión*. Según la definición

$A \subset B \leftrightarrow$ (Para cada $x, x \in A \rightarrow x \in B$).

El conjunto A se denomina*subconjunto* propio del conjunto B si $A \subset B$ y $A \neq B$. La notación $A \underset{\neq}{\subset} B$ significa que A es el subconjunto propio del conjunto B.

Nótese las propiedades de la relación de inclusión que se deducen fácilmente de la definición:

(a) La relación de inclusión es *reflexiva*, es decir $A \subset A$ para todo conjunto A;
(b) La relación de inclusión es *transitiva*, es decir que para los conjuntos A, B, C, se deduce de $A \subset B$ y $B \subset C$ que $A \subset C$;
(c) La relación de inclusión es *anti simétrica*, es decir que para los conjuntos A, B, C se deduce $A \subset B$ y $B \subset A$ que $A = B$.

Se deriva de la propiedad (c) que para establecer la igualdad de conjuntos Ay B basta demostrar que $A \subset B$ y $B \subset A$, es decir

$(A = B) \leftrightarrow (A \subset B \wedge B \subset A)$.

En teoría de conjuntos se adopta el siguiente principio para la separación de subconjuntos de un conjunto dado con el oficio de predicados monódicos: *para todo conjunto A y predicado monádico $P\ (x)$ significativo para todos los elementos del conjunto A* (es decir, tal que, para toda x de A, $P\ (x)$ es verdadero o falso) *existe un conjunto compuesto exactamente de elementos del conjunto A para los cuales $P\ (x)$ es verdadero*.

Este conjunto se denota así:

$\{x \in A \mid P\ (x)\text{es verdadero}\}$, o de manera más concisa:$\{x \in A \mid P\ (x)\}$.

La última notación se lee: «el conjunto de tal x de A que $P\ (x)$ sea valido» o «el conjunto de tal x de A para los cuales $P(x)$ es verdadero». A veces para denominar este conjunto se utiliza la notación:

$\{x \mid x \in A \wedge\ P\ (x)\}$.

Si dos predicados monádicos $P\ (x)\ y\ Q\ (x)$ son equivalentes, entonces, conforme a la definición de la igualdad de conjuntos, se define un mismo subconjunto del conjunto A, es decir que de la equivalencia $P\ (x)\ \equiv Q\ (x)$ se despeja la igualdad

$\{x \in A \mid P\ (x)\} = \{x \in A \mid Q\ (x)\}$.

Conjunto vacío. Se introduce una nueva noción importante.

DEFINICIÓN. Un conjunto que no contiene ningún elemento se denomina *conjunto vacío*.

Así, el conjunto A se denomina vacío si para cualquier $xx \notin A$ puesto que el conjunto es único. En efecto, si C y D son conjuntos vacios, entonces se tiene para cada x la equivalencia $x \in C\ \leftrightarrow x \in D$, dado que sus dos términos son falsos. Según la definición de igualdad de conjunto se deduce que $C = D$.

El conjunto vacío único se denota por el símbolo ∅, el cual para cada $xx\ \notin\ \emptyset$.

PROPOSICIÓN 1.1 *un conjunto vacío es un subconjunto de cualquier conjunto*.

Demostración. En efecto, sea A un conjunto cualquiera para cada x se verifica la implicación $x \in \emptyset \rightarrow$ x ∈ A, ya que una implicación en premisa falsa es verdadera. Por consiguiente, $\emptyset \subset$ A. □

Operaciones con conjuntos. Estúdiese las operaciones con conjuntos que permiten obtener conjuntos nuevos a partir de dos conjuntos cualesquiera.

DEFINICIÓN. Se denomina *unión de dos conjuntos* A y B al conjunto compuesto de únicos elementos que pertenecen al menos a uno de los conjuntos A y B y solamente de ellos.

El conjunto existe siempre.

De la definición de igualdad de dos conjuntos se deduce que para los conjuntos A y B existe un conjunto único que constituye su reunión. Y de hecho, si existieran dos conjuntos tales como C y D, serían compuestos de los mismos elementos y; que por lo tanto, deberían coincidir.

Este conjunto único, unión de conjuntos A y B, se denota $A \cup B$. Así mismo, por definición,

$A \cup B = \{x \mid x \in A\ \vee x \in B\ \}$.

Por consiguiente, para un x cualquiera se tiene la equivalencia

$x \in A \cup B\ \leftrightarrow x\ \in A \vee x \in B$.

De la definición de unión de conjuntos se desprende igualmente que

$A \subset A \cup B$ y$B \subset A\ \cup B$.

Ejemplo. Si $A = \{1, 9, 18\}$ y $B = \{1, 5, 9\}$, entonces $A \cup B = \{1, 5, 9, 18\}$.

DEFINICIÓN. Se denomina *intersección de conjuntos* A y B al conjunto compuesto de elementos comunes en A y B y solamente de ellos.

El conjunto existe siempre.

Para dos conjuntos cualquiera A y B existe un conjunto único que constituye su intersección. Y de hecho, si existiesen dos conjuntos C y D, entonces contendrían los mismos elementos y; por consiguiente, coincidirían la intersección de los conjuntos A y B se denota por $A \cap B$. La cual, por definición

$A \cap B = \{x \mid x \in A \wedge x \in B\}$.

Por consecuencia, para un x cualquiera se obtiene la equivalencia

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$$

Se deduce la definición de la intersección de conjuntos que

$A \cap B \subset A$y$A \cap B \subset B$.

Ejemplo. Si $A = \{1/2, 2/3, 5/6\}$, $B = \{1, 3/2, 1/2\}$ entonces $A \cap B = \{1, 2\}$

DEFINICIÓN. Se denomina *diferencia de conjuntos*A y B al conjunto formado de elementos del conjunto A que no pertenecen al conjunto B y solamente de ellos.

Para conjuntos cualquieras A y B se tiene siempre un tal conjunto y es único. La diferencia de conjuntos A y B se denota $A \setminus B$. La cual por definición,

$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

Por consiguiente, para un x cualquiera tiene la equivalencia

$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$.

Ejemplo. Si $A = \{6,9,12,13\}$,$B = \{6, 9, 10\}$, entonces $A \setminus B = \{12, 13\}$.

TEOREMA 1.2. *Para conjuntos cualquieras A y B las tres relaciones siguientes son equivalentes:*

(a) $A \subset B$; (b) $A \cup B = B$; (c) $A \cap B = A$.

Demostración.$(a) \rightarrow (b)$.Cada elemento del conjunto $A \cup B$ pertenece a A o B y en virtud de (a), es un elemento del conjunto B, es decir $A \cup B \subset B$. Además, $B \subset A \cup B$; por consiguiente, $A \cup B = B$;

$(a) \rightarrow (c)$. En virtud de (a) cada elemento del conjunto A es un elemento común de A y B, es decir $A \subset A \cap B$. Además,$A \cap B \subset A$; por consiguiente, $A \cap B = A$;

$(b) \rightarrow (c)$. Se tiene $A \subset A \cup B$ y en virtud de (b), $A \cup B \subset B$, también $A \subset B$. Como $(a) \rightarrow (c)$, tiene la igualdad (c);

$(c) \rightarrow (a)$. En virtud de (c) $A \subset A \cap B$. También tiene $A \cap B \subset B$; por consiguiente, $A \subset B$. □

Propiedades principales de operaciones con conjuntos.Las operaciones unión e intersección con conjuntos poseen una serie de propiedades. Se hará una revisión de las principales propiedades de las operaciones.

TEOREMA 1.3. *Se obtiene para conjuntos cualquieras A, B y C*

(1)$A \cup A = A$ *idempotencia de la unión;*

(2)$A \cap A = A$ *idempotencia de la intersección;*

$(3)A \cup B = B \cap A$ *conmutatividad de la unión*

$(4)A \cap B = B \cap A$ *conmutatividad de la intersección;*

(5) $A \cup (B \cup C) = (A \cup B) \cup C$ *asociativa de la unión;*

(6) $A \cap (B \cap C) = (A \cap B) \cap C$ *asociativa de la intersección;*

(7) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *distributividad de la unión sobre la intersección;*

(8) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *distributividad de la intersección sobre la unión.*

Demostración. Las cuatros primeras propiedades de idempotencia y conmutatividad se deducen fácilmente de la definición de operaciones de unión e intersección. Para demostrar la propiedad asociativa (5) basta notar que $A \cup (B \cup C)$ es un conjunto de elementos que pertenecen al conjunto A o al conjunto B, o al conjunto C, en cuanto al conjunto $(A \cup B) \cup C$, esta compuesto de los mismos elementos. De manera análoga se demuestra la propiedad (6).

Demuéstrese la propiedad (7). Sea

$$D = A \cup (B \cap C), E = (A \cup B) \cap (A \cup C).$$

Se debe demostrar que los conjuntos D y E son iguales, es decir: (a) si $x \in D$, entonces $x \in E$; (b) si $x \in E$,entonces $x \in D$.

Sea $x \in A \cup (B \cap C)$. Se presentan dos casos:

$(a_1)\ x \in A$y$(a_2)\ x \in B \cap C$.

Si $(a_1)\ x \in A \cup B$ y $x \in A \cup C$; por consiguiente, $x \in E$. Si $(a_2)\ x \in B$ y $x \in C$, de manera que $A \cup Cx \in A \cup B$y $x \in A \cup C$, por consiguiente, $x \in E$.

Supóngase ahora que $x \in E$, es decir que $x \in (A \cup B) \cap (A \cup C)$, entonces

$x \in A \cup B$y$x \in A \cup C$.

Además, si $x \notin A$, entonces $x \in B$ y $x \in C$, de manera que $x \in B \cap C$; por consiguiente, $x \in A \cup (B \cap C)$. Si por el contrario $x \in A$, entonces $x \in A \cup (B \cap C)$, es decir $x \in D$. De A y B se deduce la igualdad (5).

La propiedad de distributividad (8) se demuestra de manera análoga. □

Conjunto universal: Complementario de un conjunto. En número de aplicaciones de la teoría de conjuntos solo se considera que los conjuntos incluidos en un cierto conjunto fijo. Por ejemplo, en geometría tiene relación conjuntos de puntos de un espacio dado, en aritmética elemental subconjuntos de conjunto de todos los enteros.

En la sucesión del planteamiento las letras $A, B,\ldots$ se representa siempre los conjuntos incluidos en un cierto conjunto fijo que se denominará *conjunto universal* y se denota U. Cuyo se considera que para todo conjunto A se tiene $A \subset U$. Por consiguiente, para cada conjunto A:

(1) $A \cup U = U, \quad A \cap U = A.$

DEFINICIÓN: El conjunto $U \setminus A$ se denomina *complementario del conjunto*A y se denota A' (o $\bar{A}$). El complementario $U \setminus A'$ del conjunto A' se denota A'' (o A^C).

Se ve fácilmente que

(2) $A \cup A' = U, \quad A \cap A' = \emptyset.$

PROPOSICIÓN 1.4. *Para todo conjunto*A

(3) $A'' = A$ (ley de involución).

Se deja al criterio del lector esbozar la Demostración.

PROPOSICIÓN 1.5. $Si\ A \subset B, entonces\ B' \subset A'$.

Demostración. Sea $A \subset B$. Se debe demostrar que para toda x de U si $x \in B'$, se tiene $x \in A'$. En efecto, si $x \in B'$, entonces $x \notin B$. Teniendo en cuenta la condición $A \subset B$, se concluye que $x \notin A$ y $x \in A'$. □

TEOREMA1.6. *Se tiene las identidades siguientes*:

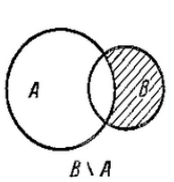
(Leyes de Morgan aplicadas a los conjuntos).

$$\left.\begin{array}{l}(4)(A \cup B)' = A' \cap B' \\ (5)(A \cap B)' = A' \cup B'\end{array}\right\}$$

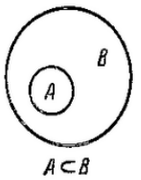
Demostración. Muéstrese que para toda x se tiene

$$(6) \quad x \in (A \cup B)' \leftrightarrow x \in A' \cap B'.$$

De hecho, $x \in (A \cup B)'$ si y solo si $x \notin A \cup B$. Pero $x \notin A \cup B$ si y solo si $x \notin A$ y $x \notin B$, es decir si $x \in A'$ y $x \in B'$ y, por consiguiente, $x \in A' \cap B'$.



$B \setminus A$



$A \subset B$

La identidad (5) se demuestra de la manera siguiente. Al utilizar la identidad (4) y la ley de involución, se obtiene

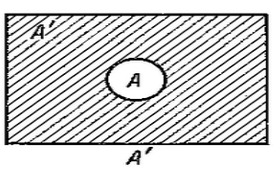
$$(A' \cup B') = A'' \cap B'' = A \cap B.$$

Por consiguiente,

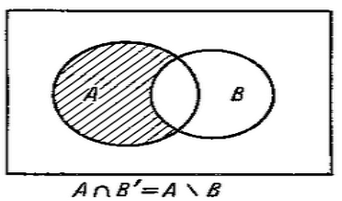
$$(A \cap B) = (A' \cup B')' = A' \cup B',$$

Es decir que la identidad (5) es verdadera. □

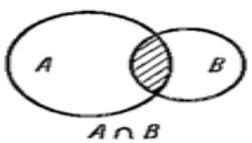
Diagrama de Euler-Venn. Para la representación gráfica de los conjuntos y sus propiedades se utiliza los d i a g r a m a s de E u l e r llamados igualmente d i a g r a m a s d e V e n n. Un conjunto se representa por un círculo (o por cualquier figura cerrada) en un plano y se supone que constituye el conjunto de los puntos del círculo. Si se representa por círculos los conjuntos A y B, los conjuntos $A \cap B$ y $A \cup B$ corresponderán a las partes rayadas



A'



$A \cap B' = A \setminus B$



$A \cap B$

Fig.1

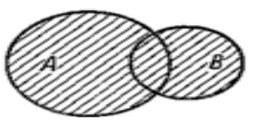


Fig.2

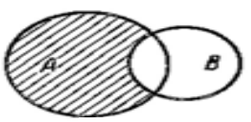


Fig.3

(fig. 1 y 2). Los conjuntos $A \setminus B$ y $B \setminus A$ se reflejarán respectivamente en los diagramas de las figuras 3 y 4. La relación $A \subset B$ se representa en la figura 5.

Fig.4 Fig.5

El conjunto universal U se figura por el conjunto de puntos de un rectángulo. El complementario A' del conjunto A hasta U

Fig.6 Fig.7

Es la parte rayada del rectángulo (fig.6) que se encuentran en el exterior del círculo del conjunto A. La igualdad $A \setminus B = A \cap B'$ se ilustra en la figura 7.

Ejercicios

1. Demostrar las identidades siguientes:

(a) $A \setminus B = A \cap B'$;
(b) $A \setminus (A \setminus B) = A \cap B$;
(c) $B \cup (A \setminus B) = A \cup B$;
(d) $B \cap (A \setminus B) = \emptyset$;
(e) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(f) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Representar las identidades por medio de diagramas de Euler-Venn.

2. Mostrar con ejemplos que las fórmulas siguientes no son siempre verdaderas:

(a) $(A \cup B) \setminus B = A$; (b) $A \setminus B \cup B = A$.

3. Demostrar las afirmaciones siguientes:

(a) $B \subset A \rightarrow (A \setminus B) \cup B = A$;
(b) $A \subset B \equiv A \cap B \equiv A$;
(c) $A \subset B \equiv A \cup B \equiv A$;
(d) $A \cap B = \emptyset \rightarrow (A \cup B) \setminus B = A$;
(e) $A \subset B \rightarrow A \setminus C \subset B \setminus C$;
(f) $A \subset B \rightarrow A \cap C \subset B \cap C$;
(g) $A \subset B \rightarrow A \cup C \subset B \cup C$;
(h) $B \subset A \wedge C = A \setminus B \rightarrow A = B \cup C$;
(i) $A \not\subset B \wedge B \cap C = \emptyset \rightarrow A \cup C \not\subset B \cup C$;
(k) $C = A \setminus B \rightarrow B \cap C = \emptyset$;
(l) $A \not\subset B \rightarrow A \setminus B \neq \emptyset$;
(m) $B \cap C = \emptyset \wedge A \cap C \neq \emptyset \rightarrow A \setminus B \neq \emptyset$;
(n) $A \subset C \rightarrow A \cup (B \cap C) = (A \cup B) \cap C$.

Ilustrar las afirmaciones por medio de diagramas de Euler-Venn.

4. Demostrar las equivalencias siguientes:

(a) $A \cup B = \emptyset \equiv A = \emptyset \wedge B = \emptyset$;
(b) $A \setminus B = A \equiv B \setminus A = B$;
(c) $A \cup B = A \setminus B \equiv B = \emptyset$;
(d) $A \setminus B = A \cap B \equiv A = \emptyset$;
(e) $A \cup B \subset C \equiv A \subset C \wedge B \subset C$;
(f) $C \subset A \cap B \equiv C \subset A \wedge C \subset B$;
(g) $A \subset B \cup C \equiv A \setminus B \subset C$;
(h) $A \cap B = A \cup B \equiv A = B$;
(i) $A \subset B \subset C \equiv A \cup B = B \cap C$.

5. Sea A y B conjuntos finitos. Demostrar que n $(A \cap B) = n(A) + n\,(B) - n(A \cap B)$, donde $n\,(M)$ es el número de elementos del conjunto M.
6. Demostrar que el conjunto compuesto de n elementos poseen 2^nsubconjuntos diferentes.
7. Mostrar que para $m < n$ el conjunto compuesto de n elementos posee $\frac{n!}{(n-m)!(m!)}$ subconjuntos diferentes a m elementos (donde $m! = 1.2 \ldots m$).
8. Sean A ($\boldsymbol{x}$) y B ($\boldsymbol{x}$) los predicados monódicos y $\boldsymbol{U}$ el dominio de valores específicos de la variable $\boldsymbol{x}$. Demuéstrese entonces que:

$\{\boldsymbol{x}|\boldsymbol{A} \vee \boldsymbol{B}\,(\boldsymbol{x})\} = \{\boldsymbol{x}|\boldsymbol{A}(\boldsymbol{x})\} \cup \{\boldsymbol{x}|\boldsymbol{B}\,(\boldsymbol{x})\}$;

$\{x|\ \boldsymbol{A}(\boldsymbol{x}) \wedge \boldsymbol{B}\,(\boldsymbol{X})\} = \{\boldsymbol{x}|\boldsymbol{A}(\boldsymbol{x})\} \cap \{\boldsymbol{x}|\boldsymbol{B}(\boldsymbol{x})\}$;

$\{\boldsymbol{x}|\neg\boldsymbol{A}(\boldsymbol{x})\} = \boldsymbol{U}\backslash\{\boldsymbol{x}|\boldsymbol{A}\,(\boldsymbol{x})\} = \{\boldsymbol{x}|\boldsymbol{A}(\boldsymbol{x})\}'$;

$\{\boldsymbol{x} \mid \boldsymbol{A}\,(\boldsymbol{x}) \rightarrow \boldsymbol{B}(\boldsymbol{x})\} = \{\boldsymbol{x} \mid \boldsymbol{A}(\boldsymbol{x})\}' \cup \{\boldsymbol{x}|\boldsymbol{B}\,(\boldsymbol{x})\}$;

$\boldsymbol{x} \mid \boldsymbol{A}\{\,(\boldsymbol{x}) \leftrightarrow \boldsymbol{B}(\boldsymbol{x})\} = (\{\boldsymbol{x} \mid \boldsymbol{A}(\boldsymbol{x})\}' \cap \{\boldsymbol{x} \mid \boldsymbol{B}(\boldsymbol{x})\}') \cup (\{\boldsymbol{x} \mid \boldsymbol{A}(\boldsymbol{x})\} \cap$

$\cap\ \{\boldsymbol{x} \mid \boldsymbol{B}(\boldsymbol{x})\})$.

§ 2. Relaciones binarias

El producto cartesiano de conjuntos. Sean dados cualquiera de los objetos a y b. Si a ≠b, el conjunto {a, b} se denomina *par no ordenado de objetosa* y b. Nótese que siempre se tiene $\{\{a, b\} = \{b, a\}$.

Introdúzcase una nueva noción elemental, la noción de pares ordenados. Asóciese a dos objetos a yb un nuevo objeto constituido por su par ordenado $\langle a, b\rangle$.

DEFINICIÓN: Las pares ordenado$\langle a, b\rangle$ y $\langle c, d\rangle$se denominan *iguales* y se escriben $\langle a, b\rangle = \langle c, d\rangle$ si y solo si $a = c$ y $b = d$.

En particular, $\langle a, b\rangle = \langle b, a\rangle$ si y solo si $a = b$.

En consecuencia se dirá frecuentemente << par $\langle a, b\rangle$>> en lugar de << par ordenado $\langle a, b\rangle$>>. Al elemento a se le llama *primer elemento de par*$\langle a, b\rangle$, mientras que b es el *segundo elemento del par*.

DEFINICIÓN: Llámese *producto cartesiano de conjuntos* $\boldsymbol{A}$ *y* $\boldsymbol{B}$ al conjuntos de todos los pares ordenados $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ tal como $\boldsymbol{x} \in \mathbf{A}y\mathbf{Y} \in \boldsymbol{B}$.

Se denota a este conjunto $\boldsymbol{A}\ \boldsymbol{X}\ \boldsymbol{B}$.

Por lo tanto:

$\boldsymbol{AXB} = \{\langle \boldsymbol{x}, \boldsymbol{y}\rangle | \boldsymbol{x} \in \boldsymbol{A}\ \forall \wedge \boldsymbol{y} \in \boldsymbol{B}\}$.

$\boldsymbol{E}$Jemplo: Sean $\boldsymbol{A} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$y $\boldsymbol{B} = \{\mathbf{3}, \mathbf{5}\}$. Entonces se tiene $\boldsymbol{A} \times \boldsymbol{B} = \{\langle \mathbf{0}, \mathbf{3}\rangle, \langle \mathbf{0}, \mathbf{5}\rangle, \langle \mathbf{1}, \mathbf{3}\rangle, \langle \mathbf{1}, \mathbf{5}\rangle, \langle \mathbf{2}, \mathbf{3}\rangle, \langle \mathbf{2}, \mathbf{5}\rangle\}$;

$\boldsymbol{B} \times \boldsymbol{A} = \{\langle 3,0\rangle, \langle \mathbf{5}, \mathbf{0}\rangle, \langle \mathbf{3}, \mathbf{1}\rangle, \langle \mathbf{5}, \mathbf{1}\rangle, \langle \mathbf{3}, \mathbf{2}\rangle, \langle \mathbf{5}, \mathbf{3}\rangle\}$;

$\mathbf{A} \times \mathbf{A} = \{\langle 0,0\rangle, \langle \mathbf{0}, \mathbf{1}\rangle, \langle \mathbf{0}, \mathbf{2}\rangle, \langle \mathbf{1}, \mathbf{1}\rangle, \langle \mathbf{1}, \mathbf{0}\rangle, \langle \mathbf{1}, \mathbf{2}\rangle,$

$\langle \mathbf{2}, \mathbf{0}\rangle, \langle \mathbf{2}, \mathbf{1}\rangle, \langle \mathbf{2}, \mathbf{2}\rangle\}$;

$\mathbf{B} \times \mathbf{B} = \{\langle 3,3\rangle, \langle \mathbf{3}, \mathbf{5}\rangle, \langle \mathbf{5}, \mathbf{5}\rangle, \langle \mathbf{5}, \mathbf{3}\rangle\}$.

La noción generalizada de par ordenado es la noción de sucesión (serie ordenado) de n objetos. La sucesión de n objetos$\langle \mathbf{a_1}, \ldots, \boldsymbol{a_n} \rangle$ se denota $\langle \mathbf{a_1}, \ldots, \boldsymbol{a_n} \rangle$.

DEFINICIÓN: Dos sucesiones $\langle \mathbf{a_1}, \ldots, \boldsymbol{a_n} \rangle$ y$\langle \mathbf{b_1}, \ldots, \boldsymbol{b_n} \rangle$ se denominan *iguales* y se escriben $\langle \mathbf{a_1}, \ldots, \boldsymbol{a_n} \rangle = \langle \mathbf{b_1}, \ldots, \boldsymbol{b_n} \rangle$ Si, y solo si,$\mathbf{a_1} = \mathbf{b_1}$,. . ., $\mathbf{a}_n = \boldsymbol{b_n}$.

Se denominan tripletas ordenados a las sucesiones de tres objetos. S e llama *producto cartesiano de tres conjuntos* a $\boldsymbol{A}$, $\boldsymbol{B}$ Y $\boldsymbol{C}$ al conjunto de todas las tripletas ordenadas$\langle \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \rangle$ tal como $x \in \boldsymbol{A}$, y $\in$ $\boldsymbol{B}$ y $\boldsymbol{z} \in \boldsymbol{C}$.

Este conjunto se denota$\boldsymbol{A} \times \boldsymbol{B} \times \boldsymbol{C}$; por tanto:

$\boldsymbol{A} \times \boldsymbol{B} \times \boldsymbol{C} = \{\langle \boldsymbol{x}, \boldsymbol{z}, \boldsymbol{y} \rangle \mid \boldsymbol{x} \in \boldsymbol{A}, \text{Y} \in \boldsymbol{B} \text{ y } \boldsymbol{z} \in \boldsymbol{C}\}$.

Sean $\boldsymbol{A}$ un conjunto no vacío y n un entero positivo. Se denota a $\boldsymbol{A^n}$el conjunto de sucesiones$\langle \boldsymbol{x_1}, \ldots, \boldsymbol{x_n} \rangle$ de elementos de $\boldsymbol{A}$, quiere decir que:

$\boldsymbol{A^n} = \langle \boldsymbol{x_1}, \ldots, \boldsymbol{x_n} \rangle \mid \boldsymbol{x_1} \in \boldsymbol{A}, \ldots, \boldsymbol{x_n} \in \boldsymbol{A}\}$.

Supongamos que$\boldsymbol{A^1} = \boldsymbol{A}$ .El conjunto$\boldsymbol{A^n}$se denomina$n$- uplas producto cartesiano del conjunto $\boldsymbol{A}$ a la potencia $\boldsymbol{n}$ – esima del conjunto $\boldsymbol{A}$ .En particular, $\boldsymbol{A^2} = \boldsymbol{A} \times \boldsymbol{A}$ y $\boldsymbol{A^3} = \boldsymbol{A} \times \boldsymbol{A} \times \boldsymbol{A}$.

DEFINICIÓN: Llámese *producto cartesiano* de $\boldsymbol{n}$ conjuntos $\mathbf{A_1}, \ldots, \boldsymbol{B_n}$al conjunto de sucesiones de longitud de $\boldsymbol{n}\langle \boldsymbol{x_1}, \ldots, \boldsymbol{x_n} \rangle$tales como $\boldsymbol{x_1} \in \boldsymbol{A_1}, \ldots, \boldsymbol{x_n} \in \boldsymbol{A_n}$.

El producto cartesiano de conjuntos $\boldsymbol{A_1}, \ldots, \boldsymbol{A_n}$ se denota por el símbolo $\boldsymbol{A_1} \times \ldots \times \boldsymbol{A_2} \times \ldots \times \boldsymbol{A_n}$;por tanto, $\boldsymbol{A_1} \times \ldots \times \boldsymbol{A_n} = \times \ldots \times \boldsymbol{A_n} \{\langle \boldsymbol{x_1}, \ldots, \boldsymbol{x_n} \rangle \mid \boldsymbol{x_1} \in \boldsymbol{A_1}, \ldots, \boldsymbol{x_n} \in \boldsymbol{A_n}\}$.

Relaciones binarias. Es una de las nociones esenciales de la teoría de conjuntos.

DEFINICIÓN. Se denomina *relaciones binarias* a todo conjuntos de pares ordenados.

De la definición se deduce que un subconjunto cualquiera del producto cartesiano de dos conjuntos es una relación binaria.

Si $\boldsymbol{R}$ es una relación binaria y $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \boldsymbol{R}$,sedice qué $\boldsymbol{x}$ y $\boldsymbol{y}$ *están unidas por la relación* $\boldsymbol{R}$ es por esta razón que el *elemento* $\boldsymbol{x}$ *se relaciona* con $\boldsymbol{R}$ y $\boldsymbol{y}$ como también $\boldsymbol{x}$ y $\boldsymbol{y}$*secumple con la relación*$\boldsymbol{R}$.En lugar de $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \boldsymbol{R}$ con frecuencia se utiliza una notación más simple:

$$\boldsymbol{xRy},$$

Empleada a su vez para señalar la afirmación que ≪los elementos $\boldsymbol{x}$ y $\boldsymbol{y}$ están relacionados por la relación $\boldsymbol{R}$ ≫.

DEFINICIÓN: Se *denomina dominio (conjunto) de definición de la relación*$\boldsymbol{R}$ al conjunto de primeros elementos de par de $\boldsymbol{R}$ y se denota $\boldsymbol{Dom\ R}$:

$\boldsymbol{Dom}=\boldsymbol{R}\ \{\ \boldsymbol{x} \mid \exists \boldsymbol{y}\ (\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \boldsymbol{R})\}$.

Se denomina *dominio de valores de relación*$\boldsymbol{R}$ al conjuntos de segundos elementos de par de $\boldsymbol{R}$ y se denota $\boldsymbol{Im\ R}$:

$\boldsymbol{ImR} = \{\ \boldsymbol{y} \mid \exists \boldsymbol{x}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \boldsymbol{R})\}$.

DEFINICIÓN: Se denomina *dominio de relación*$\boldsymbol{R}$ al conjunto $\boldsymbol{Dom\ R} \cup \boldsymbol{Im\ R}$.

Se ve sin duda que:

$\boldsymbol{R} \subset \boldsymbol{DomR}$ X $\boldsymbol{ImR}$.

$\boldsymbol{Si\ R} \subset \boldsymbol{A}$ X $\boldsymbol{B}$, se dice que $\boldsymbol{R}$ es la *relación entre los elementos de conjuntos* $\boldsymbol{A}$ Y $\boldsymbol{B}$ o que $\boldsymbol{R}$*esta definido por una pare de conjuntos* de $\boldsymbol{A}$ X $\boldsymbol{B}$.

Si $\boldsymbol{A} \subset \boldsymbol{C}\ \boldsymbol{y}\ \boldsymbol{B} \subset \boldsymbol{D}$, se tiene $\boldsymbol{R} \subset \boldsymbol{C}$ X $\boldsymbol{D}$, quiere decir que $\boldsymbol{R}$ es igual a la las relación entre los elementos de conjuntos $\boldsymbol{C}\ \boldsymbol{y}\ \boldsymbol{D}$.Si $\boldsymbol{R} \subset \subset \boldsymbol{A}$ X $\boldsymbol{B}$,entonces el $\boldsymbol{Dom\ R\ A} \subset \boldsymbol{A}$ y $\boldsymbol{Im\ R} \subset \boldsymbol{B}$.Cada relación $\boldsymbol{R}$ es una relación entre los elementos de conjuntos de $\boldsymbol{Dom\ R}$ y $\boldsymbol{Im\ R}$.

DEFINICIÓN: Si $\boldsymbol{R} \subset \boldsymbol{A}$ X $\boldsymbol{A}$, se denomina que $\boldsymbol{R}$ es *una relación binaria* en el conjunto $\boldsymbol{A}$.

Es claro que cada relación binaria $\boldsymbol{R}$ es una relación en el dominio de la relación $\boldsymbol{R}$.

DEFINICIÓN: Las relaciones binarias $\boldsymbol{R}\ \boldsymbol{y}\ \boldsymbol{S}$ se denominan *iguales* si, y solo si, $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \boldsymbol{S}$ para todos $\boldsymbol{x}, \boldsymbol{y}\ \langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \boldsymbol{R}$, quiere decir que si $\boldsymbol{R}\ \boldsymbol{y}\ \boldsymbol{S}$ son iguales como conjuntos.

DEFINICIÓN: Sean $\boldsymbol{R}\ \boldsymbol{y}\ \boldsymbol{S}$ relaciones binarias. Se denomina *composición (o superposición*) *de relaciones* al conjunto de todas las parejas de $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ tal que para un cierto $\boldsymbol{z}\ \langle \boldsymbol{x}, \boldsymbol{z}\rangle \in \boldsymbol{S}$ y $\langle \boldsymbol{z}, \boldsymbol{y}\rangle \in \boldsymbol{R}$ y se denota: $\boldsymbol{R} \circ \boldsymbol{S}$.

Por definición, se tiene:

$\boldsymbol{R} \circ \boldsymbol{S} = \{\langle \boldsymbol{x}, \boldsymbol{y}\rangle \mid \exists \mathbf{z}\ (\boldsymbol{x}, \boldsymbol{y}\boldsymbol{S}\boldsymbol{z} \wedge \boldsymbol{z}\boldsymbol{R}\boldsymbol{y})\}$.

Ejemplo: Si $\boldsymbol{S} = \{\langle \mathbf{1}, \mathbf{2}\rangle, \langle \mathbf{2}, \mathbf{4}\rangle, \langle \mathbf{3}, \mathbf{6}\rangle\}$ $\boldsymbol{R} = \{= \{\langle \mathbf{1}, \mathbf{3}\rangle,$

$\{\langle \mathbf{2}, \mathbf{6}\rangle, \langle \mathbf{3}, \mathbf{9}\rangle, \langle \mathbf{4}, \mathbf{12}\rangle\}$, entonces $\boldsymbol{R} \circ \boldsymbol{S} = \{\langle \mathbf{1}, \mathbf{6}\rangle, \langle \mathbf{2}, \mathbf{12}\rangle\}$.

DEFINICIÓN: Se denomina *inversa* de la relación binaria $\boldsymbol{R}$ al conjunto de todas las parejas ordenados de $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ tales que $\langle \boldsymbol{y}, \boldsymbol{x}\rangle \in \boldsymbol{R}$.

La inversa de la relación $\boldsymbol{R}$ se denota $\boldsymbol{R}^{\smile}$.Por lo tanto, por definición,

$\boldsymbol{R}^{\smile} = \{\langle \boldsymbol{x}, \boldsymbol{y}\rangle \mid \langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \boldsymbol{R}\}$.

Ejemplo: Si $\boldsymbol{R} = \{\langle \mathbf{2}, \mathbf{5}\rangle, \{\langle \mathbf{8}, \mathbf{15}\rangle, \langle \mathbf{4}, \mathbf{1}\rangle$,entonces $\boldsymbol{R}^{\smile} = \{\langle \mathbf{5},\ \mathbf{2}\rangle,\ \langle \mathbf{15},\ \mathbf{8}\rangle, \langle \mathbf{1},\ \mathbf{4}\rangle\}$.

PROPOSICIÓN 2.1. Si $\boldsymbol{R}$ *es una relación binaria cualquiera*, se tienen,

(a)$\boldsymbol{Dom}(\boldsymbol{R}^{\smile}) = \boldsymbol{ImR}$, (b)$\boldsymbol{Im}(\boldsymbol{R}^{\smile}) = \boldsymbol{DomR}$, (c) $(\boldsymbol{R}^{\smile})^{\smile} = \boldsymbol{R}$,

Es decir que si $\boldsymbol{R}^{\smile}$ es una inversa de $\boldsymbol{R}$, recíprocamente, $\boldsymbol{R}$ es la inversa de $\boldsymbol{R}^{\smile}$.

Esta proposición se deduce directamente de la definición de la inversa de $\boldsymbol{R}^{\smile}$ de la relación $\boldsymbol{R}$.

DEFINICIÓN: La relación $\boldsymbol{R}$ se denomina *restricción* de la relación $\boldsymbol{S}$ y $\boldsymbol{S}$ *extensión* de $\boldsymbol{R}$, si $\boldsymbol{R} \subset \boldsymbol{S}$.

DEFINICIÓN: La relación binaria $\boldsymbol{R}$ se denomina *restricción de la relación* $\boldsymbol{S}$ por el conjunto $\boldsymbol{A}$, si $\boldsymbol{R} = (\boldsymbol{A} \times \boldsymbol{A}) \cap \boldsymbol{S}$.

Si la relación binaria $\boldsymbol{R}$ es una restricción de la relación $\boldsymbol{S}$ por el conjunto $\boldsymbol{A}$, $\boldsymbol{R}$ es recíprocamente la restricción de $\boldsymbol{S}$ y $\boldsymbol{Dom}\ \boldsymbol{R} \subset \boldsymbol{A}$.

TEOREMA 2.2. *La composición de relaciones se asocia a la propiedad asociativa*, es decir que para todas las relaciones binarias $\boldsymbol{R}, \boldsymbol{S}, \boldsymbol{T}$ se tiene:

(1) $(\boldsymbol{R} \circ \boldsymbol{S}) \circ \boldsymbol{T} = \boldsymbol{R} \circ (\mathbf{S} \circ \mathbf{T})$.

Demostración. Para todos $\boldsymbol{x}$ y $\boldsymbol{y}$ se tiene:

$$\boldsymbol{\chi}(\boldsymbol{R} \circ \boldsymbol{S}) \circ \boldsymbol{T}\boldsymbol{y} \leftrightarrow \exists \mathbf{z}(\boldsymbol{\chi}\ \mathbf{T}\ \boldsymbol{\mathcal{Z}} \wedge \mathbf{z}\ \mathbf{R} \circ \boldsymbol{S}\boldsymbol{y})$$
$$\leftrightarrow \exists \mathbf{z} \exists\ \boldsymbol{t}\ (\boldsymbol{\chi}\ \mathbf{T}\ \boldsymbol{\mathcal{Z}} \wedge\ \mathbf{z}\ \boldsymbol{S}\ \boldsymbol{t} \wedge \mathbf{t}\ \mathbf{R}\ \boldsymbol{y})$$
$$\leftrightarrow \exists \mathbf{t} \exists \boldsymbol{z}\ (\boldsymbol{x}\boldsymbol{T}\boldsymbol{z} \wedge\ \mathbf{z}\ \boldsymbol{S}\boldsymbol{t}\ \wedge \mathbf{t}\ \mathbf{R}\ \boldsymbol{y})$$
$$\leftrightarrow\ \exists \mathbf{t}\ [\exists \mathbf{z}\ (\boldsymbol{x}\ \mathbf{T}\ \mathbf{z}\ \wedge\ \mathbf{z}\ \boldsymbol{S}\ \boldsymbol{t}\ \wedge\ \mathbf{t}\ \mathbf{R}\ \boldsymbol{y}]$$
$$\leftrightarrow\ \exists \mathbf{t}\ [\boldsymbol{x}\boldsymbol{S} \circ \boldsymbol{T}\mathbf{t} \wedge\ \mathbf{t}\ \mathbf{R}\ \boldsymbol{y}]$$
$$\leftrightarrow\ \boldsymbol{x}\ \boldsymbol{R} \circ\ (\boldsymbol{R} \circ \boldsymbol{T})\ \boldsymbol{y}.$$

Por lo tanto, la igualdad (1) es verdadera para todas las relaciones binarias $\boldsymbol{R}$, $\boldsymbol{S}$ y $\mathbf{T}$. □

TEOREMA 2.3. *Para todas las relaciones binarias* $\boldsymbol{R}\ \boldsymbol{y}\ \boldsymbol{S}(\boldsymbol{R} \circ\ \boldsymbol{S})^{\smile} = \boldsymbol{S}^{\smile} \circ\ \boldsymbol{R}^{\smile}$.

Demostración. Para todos $\boldsymbol{x}$ y $\boldsymbol{y}$ se tiene:

$$\boldsymbol{x}(\boldsymbol{R} \circ\ \boldsymbol{S})^{\smile}\ \boldsymbol{y} \leftrightarrow \boldsymbol{y}\boldsymbol{R}\ \circ\ \boldsymbol{S}\boldsymbol{x}$$
$$\leftrightarrow\ \exists \mathbf{z}\ (\mathbf{y}\mathbf{S}\mathbf{z} \wedge \mathbf{z}\ \mathbf{R}\ \boldsymbol{x}\ )$$
$$\leftrightarrow\ \exists \mathbf{z}\ (\boldsymbol{x}\boldsymbol{R}^{\smile}\boldsymbol{z} \bigwedge\ \mathbf{z}\boldsymbol{S}^{\smile}\boldsymbol{y})$$
$$\leftrightarrow\ \boldsymbol{x}\boldsymbol{S}^{\smile} \circ \boldsymbol{R}^{\smile}\boldsymbol{y}.$$

Por lo tanto, $(\boldsymbol{R} \circ\ \boldsymbol{S})^{\smile} = \boldsymbol{S}^{\smile} \circ\ \boldsymbol{R}^{\smile}$para todas las relaciones binarias $\boldsymbol{R}\ \boldsymbol{y}\ \boldsymbol{S}$. □

Relaciones n-áreas. La noción general de la relación binaria es la noción de la relación $\boldsymbol{n}$ áreas.

DEFINICIÓN: Se denomina ($\boldsymbol{n} \geq \mathbf{1}$) a todo el conjunto de sucesiones de longitud $\boldsymbol{n}$ (es decir que un conjunto cualquiera de series ordenados de $\boldsymbol{n}$ objetos).

Por lo tanto, una relación n-áreas es un subconjunto cualquiera de un producto cartesiano de $\boldsymbol{n}$ conjuntos.

Llámese también *relación binaria* a una relación que tiene dos variable, y *relación ternaria* a una relación que tiene tres variables. La relación ternaria se constituye por todo conjunto de tripletas ordenadas, es decir a todo subconjunto del producto cartesiano de tres conjuntos.

DEFINICIÓN: Sea $\boldsymbol{A^n}$ la enésima potencia de un conjunto no vacio $\boldsymbol{A}$, $\boldsymbol{n} \geq \mathbf{1}$. A todo subconjunto del conjunto $\boldsymbol{A^n}$ se le llama *relación $\boldsymbol{n}$ áreas en el conjunto $\boldsymbol{A}$*, y el numerador $\boldsymbol{n}$ *el rango de la relación*.

En particular, todo subconjunto del conjunto $\boldsymbol{A}$ es una relación a una variable (simple) en A; una relación de tres variables (ternaria) en $\boldsymbol{A}$ se constituye por todo subconjunto del conjunto $\boldsymbol{A^3}$, quiere decir que todo conjunto de tripletas ordenados de elementos del conjunto $\boldsymbol{A}$.

Sea A ($\boldsymbol{x_1}, \ldots, \boldsymbol{x_n}$) un predicado $\boldsymbol{n}$ área cualquiera de variables libres ($\boldsymbol{x_1}, \ldots, \boldsymbol{x_n}$). Se le puede asociar a una relación $\boldsymbol{n}$ área

$\boldsymbol{R}$= $\{\langle \boldsymbol{x_1}, \ldots, \boldsymbol{x_n} \rangle \mid \mathbf{A}\ (\boldsymbol{x_1}, \ldots, \boldsymbol{x_n})\}$.

La relación $\boldsymbol{R}$ se define como *grafo del predicado* A ($\boldsymbol{x_1}, \ldots, \boldsymbol{x_n}$).

Representación de relaciones binarias por medios de grafos. Se define grafo a una figura plana compuesta de un numero finito de puntos (vértices del grafo) y de líneas unidas a vértices. Una línea unida a dos vértices cualquiera del grafo se define como línea de grafo. Las líneas pueden ser rectas o curvas. Los puntos de intersección de algunas líneas de grafo pueden no constituir vértices de este último. Se define *grafo orientado* al grafo que se denota por flechas en dirección de sus líneas.

Existe un método más simple de representación por grafos orientados de relaciones binarias en conjuntos finito. Sean $\mathbf{A}$ un conjunto finito no vacio y $\boldsymbol{R}$ la relación binaria en $\mathbf{A}$, es decir que$\boldsymbol{R} \subset \boldsymbol{A}$ X $\boldsymbol{A}$ .Represéntese a los elementos del conjunto $\boldsymbol{A}$ por puntos en un plano. A cada par $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ de $\boldsymbol{R}$ para $\boldsymbol{a} \neq \boldsymbol{b}$ asóciese una línea orientada (fig.8) dirigida al punto $\boldsymbol{a}$ hacia el punto $\boldsymbol{b}$. Al par de $\langle \boldsymbol{a}, \boldsymbol{a} \rangle$ de $\boldsymbol{R}$ asóciese una curva cerrada (fig.9) con un sentidos fijo de movimientos (por ejemplo, siempre en el sentido contrario a las agujas de un reloj).Así como, a una relación binaria $\boldsymbol{R}$ se asocia a la figura geométrica siguiente: los puntos del plano que representan los elementos del conjunto $\boldsymbol{Dom\ R} \cup \boldsymbol{Im\ R}$ y las líneas orientadas, es decir que a cada par $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$de $\boldsymbol{R}$ corresponde a una línea orientada, interpuesta del punto $\boldsymbol{a}$ hacia el punto $\boldsymbol{b}$,a una curva cerrada, si $\boldsymbol{a} = \boldsymbol{b}$. Esta figura geométrica tiene por nombre *grafo orientado* de la relación $\boldsymbol{R}$ o simplemente *grafo de la relación $\boldsymbol{R}$*.

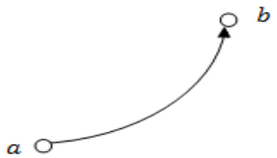


Fig. 8

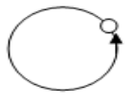


Fig. 9

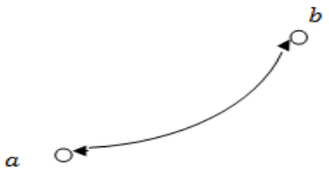


Fig.10

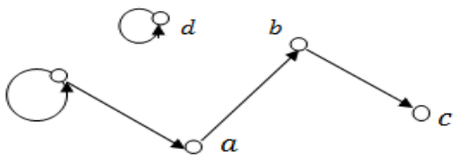


Fig.11

Si la relación $\boldsymbol{R}$ forma la pareja $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ y la pareja $\langle \boldsymbol{b}, \ \boldsymbol{a} \rangle$, entonces el grafo de la relación $\boldsymbol{R}$ tiene dos líneas y dos vértices $\boldsymbol{a}$ **y** $\boldsymbol{b}$ en sentidos opuestos. En este caso las líneas se sustituyen por una sola línea de dos flechas (Fig.10).

A La línea de dos flechas se le llama *no orientada*.

Cada relación binaria en un conjunto finito se puede representar por un grafo orientado. Inversamente, *cada grafo orientado es la representación de una relación binaria en el conjunto de sus vértices.*

E j e m p lo. La figura 11 representa el grafo de la relación

$\boldsymbol{R} = \{\langle \mathbf{a}, \mathbf{b} \rangle, \langle \mathbf{b}, \mathbf{c} \rangle, \langle \mathbf{d}, \mathbf{d} \rangle, \langle \mathbf{e}, \ \mathbf{a} \rangle, \langle \mathbf{e}, \ \mathbf{e} \rangle\}$.

Ejercicios

1. Mostrar que para todos los elementos $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}$ (estrictamente distintos)

$\{\mathbf{a}, \mathbf{b}\} = \{\mathbf{c}, \mathbf{d}\}$ Si y solo si $\mathbf{a} = \mathbf{c}$ y $\boldsymbol{b} = \boldsymbol{d}$ o $\mathbf{a} = \mathbf{d}$ y $\boldsymbol{b} = \boldsymbol{c}$.

2. Mostrar que para todos los elementos $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}$ $\{\{\boldsymbol{a}\}, \{\boldsymbol{a}, \boldsymbol{b}\}\} = \{\{\ \boldsymbol{c}\ \}, \{\boldsymbol{c}, \boldsymbol{d}\}\}$

Si y solo si $\mathbf{a} = \mathbf{c}$ y $\boldsymbol{b} = \boldsymbol{d}$.

Obsérvese. Que en virtud de esto, en par ordenado $\langle \mathbf{a}, \mathbf{b} \rangle$ con frecuencia se define en la teoría de conjuntos como en la de conjunto de $\{\{\boldsymbol{a}\}, \{\boldsymbol{a}, \boldsymbol{b}\}\}$.

3. Mostrar que $\langle\langle \mathbf{a}, \mathbf{b} \rangle, \boldsymbol{c} \ \rangle = \langle\langle \mathbf{d}, \mathbf{e} \ \rangle, \ \boldsymbol{f} \rangle$ si y solo si $\mathbf{a} = \mathbf{d}, \boldsymbol{b} = \boldsymbol{e}, \boldsymbol{c} = \boldsymbol{f}$.

4. Demostrar que para todos los conjuntos $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$:

(a) $\boldsymbol{Dom}(\boldsymbol{AXB}) = \boldsymbol{A}$;

(b) $\boldsymbol{Im}(\boldsymbol{AXB}) = \boldsymbol{B}$;

(c) $(\boldsymbol{A} \cap \boldsymbol{B})\boldsymbol{X}(\boldsymbol{C} \cap \boldsymbol{D}) = (\boldsymbol{AXC}) \cap (\boldsymbol{BXD})$;

(d) $(\boldsymbol{A} \cap \boldsymbol{B})\boldsymbol{XC} = (\boldsymbol{AXC}) \cap (\boldsymbol{BXC})$;

(e) $\boldsymbol{AX}\ (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{AXB}) \cap (\boldsymbol{AXC})$;

(f) $\boldsymbol{B} \cup \boldsymbol{C})\ \boldsymbol{XA} = (\boldsymbol{BXA}) \cup (\boldsymbol{CXA})$;

(g) $(\boldsymbol{AXB}) = \emptyset) = (\boldsymbol{A} = \emptyset \vee \boldsymbol{B} = \emptyset)$;

(h) $(\boldsymbol{A} \setminus \boldsymbol{B})$ X $\boldsymbol{C} = (\boldsymbol{AXC}) \setminus (\boldsymbol{BXC})$.

5. Mostrar por medio de ejemplos que las igualdades siguientes son verdaderas para todos los conjuntos de $\boldsymbol{A}$, $\boldsymbol{B}$ y $\boldsymbol{C}$:

($\boldsymbol{a}$) $\boldsymbol{AXB} = \boldsymbol{BXA}$;

(b) $AX(BXC) = (AXB)XC$.

6. Demostrar que para todas las relaciones binarias R, S, T se tiene:

(a) $Dom(R) = \emptyset) = (R = \emptyset) = (Im(R) = \emptyset)$;

(b) $Dom(R^{\smile}) = Im(R)$;

(c) $Im(R^{\smile}) = Dom\ )\ (R^{\smile})$;

(d) $(R^{\smile})^{\smile} = R$;

(e) $(R \circ S)^{\smile} = S^{\smile} \circ R^{\smile}$;

(f) $Dom(R \circ S) \subset DomS$;

(g) $Im(R \circ S) \subset ImR$.

7. Mostrar a través de un ejemplo que una composición de relaciones binarias no es conmutativa.

8. Buscar el $Dom\ (R), R^{\smile}, R \circ R, R \circ R^{\smile}, R^{\smile} \circ R$ para las relaciones siguientes:

(a) $R = \{\langle x, y\rangle \mid x, y \in N$ y $x$divide a $y\}$;

(b) $R = \{\langle x, y\rangle \mid x, y \in N$ y $y$divide a $x\}$;

(c) $R = \{\langle x, y\rangle \mid x, y \in Q$ y $x + y \leq 0\}$, donde Qes el conjunto de todos los Números racionales;

(d) $R = \{\langle x, y\rangle \mid x, y \in Q$y $2x \leq 3y\}$.

§ 3. Funciones

Noción de función (de Aplicación). Una de las nociones principales de las matemáticas es la noción de función.

DEFINICIÓN. Se le llama función (*Aplicación*) a la relación binaria f si para todo x, y, z se obtiene $\{\langle x, y\rangle \in f$ y $\langle x, z\rangle \in f$ como $y = z$. Dicho de otra manera, la relación f se le denomina función si para todo x del dominio de definición de la relación f existe una y única tal que para $\langle x, y\rangle \in f$. Este elemento único y se le denota $f\ (x)$ y se le llama *valor de la función* f para el argumento x.Si $\langle x, y\rangle \in f$ se usa de la notación común que $y = f(x)$,asi como de la notación $f: x \mapsto y$.

Se denomina *dominio de definición de la función* f al conjunto

$Dom\ f = \{x \mid \exists y\ (\langle x, y\rangle \in f\ )\}$.

Se denomina *dominio de valores de la función* f al conjunto

$Im\ f = \{y \mid \exists x\ (\langle x, y\rangle \in f\ )\}$.

Dos funciones f y g son iguales y (se escribe $f = g$) si f y g son iguales como conjuntos, es decir que para todo x, y $\langle x, y\rangle \in f$ si y solo si, $\langle x, y\rangle \in g$.Por consecuencia, las funciones f y g son iguales si y solo si, $Dom\ f = Dom\ g$ y $f\ (x) = g(x)$ para cada x de $Dom\ f$.

Las funciones también se llaman *aplicaciones.* Si la función f se da en la pareja de conjuntos de Ay B, es decir que si $f \subset A \times B$, se dice que f es la función de A en B. Si además $A = Dom\ f$ y $Im\ f \subset B$, Se dice que f es *la función de conjunto* A en B y se denotan

$f: A \to B$ O $A \to B$.

Si $A = Dom\ f$ y $B = Im\ f$, se dice que f es *la función de conjunto* A *en* B.

Al conjunto de todas funciones A *en* B se le designa por el símbolo B^{A}.

Llámese *imagen del conjunto* C por función f de conjunto $f\ (C) = \{f(x) \mid x \in C\}$.

Se muestra con facilidad que para todo conjunto C y toda función f.

$\boldsymbol{f}\ (\boldsymbol{C}) = \ \boldsymbol{f}\ (\mathrm{C} \cap \boldsymbol{Dom}\ \boldsymbol{f})$.

La imagen anticipada del conjunto $\boldsymbol{M}$ por función $\boldsymbol{f}$ es el conjunto

$$\boldsymbol{f}^{\smile}(\boldsymbol{M}) = \{\boldsymbol{x} \in \boldsymbol{Dom}\ \boldsymbol{f} \mid \boldsymbol{f}(\boldsymbol{x}) \in \boldsymbol{M}\},$$

es decir que el conjunto de todos los elementos $\boldsymbol{x}$ de dominio de definición de la función $\boldsymbol{f}$ para los cuales $\boldsymbol{f}\ (\boldsymbol{x}) \in \boldsymbol{M}$.Se Comprueba con facilidad que para cualquier conjunto $\boldsymbol{M}$ y una función $\boldsymbol{f}$, se cumple que

$$\boldsymbol{f}^{\smile}(\boldsymbol{M}) = \ \boldsymbol{f}^{\smile}(\boldsymbol{M} \cap\ \boldsymbol{Im}\ \boldsymbol{f}).$$

Se vio que una relación binaria se puede representar en forma de grafo de una condición de dos variables (de un predicado).Igualmente, una función se puede dar por una condición de dos variables. Sea $\boldsymbol{A}(\boldsymbol{x}, \boldsymbol{y})$ la condición de dos variables impuestas de $\boldsymbol{x}$ y $\boldsymbol{y}$, tal que no existen dos pares ordenados que satisfagan a esta condición que tuvieran sus primeros elementos idénticos sus segundos distintos. En este caso, el grafo de la condición $\boldsymbol{A}(\boldsymbol{x}, \boldsymbol{y})$, es decir que el conjunto de $\{\langle\ \boldsymbol{x}\ , \boldsymbol{y}\rangle\ \mid\ \mathbf{A}\ (\mathbf{x}, \mathbf{y})\}$,es una función.

Es así, por ejemplo que, la función definida por la condición $\boldsymbol{x^2 - y = 1}$ en el conjunto $\boldsymbol{Z}$ de enteros se puede representar como conjunto

$\boldsymbol{f} = \{\langle\ \boldsymbol{x}\ , \boldsymbol{y}\rangle \mid \boldsymbol{x},\quad \boldsymbol{y}\ \in \boldsymbol{Z}\ \ \mathrm{Y}\ \ \ \boldsymbol{x^2 - y = 1}\}$,

O por

$\boldsymbol{f} = \{\langle\ \boldsymbol{x}\ , \boldsymbol{y}\rangle \mid \boldsymbol{x},\quad\ \boldsymbol{y}\ \in \boldsymbol{Z}\ \ \mathrm{Y}\ \ \boldsymbol{y = x^2 - 1}\}$,

Y también de la forma siguiente:

$\boldsymbol{f} = \{\langle\ \boldsymbol{x}\ ,\quad \boldsymbol{x^2 - 1}\rangle \mid \boldsymbol{x},\quad\ \boldsymbol{y}\ \in\ \boldsymbol{Z}\ \}$.

Se denomina *función de dos variables*, a la función cuyo dominio de definición se compone de pares ordenados, y función de tres variables a la función de la que el dominio de definición se compone de tripletas ordenadas. Entonces si $\boldsymbol{f}$ es una función de dos variables se escriben usualmente $\boldsymbol{f}(\ \boldsymbol{x}\ , \boldsymbol{y})$ en vez de $\boldsymbol{f}\ (\boldsymbol{x}\ , \boldsymbol{y}\rangle)$.Si $\boldsymbol{f}$ es una función de tres variables se escriben $\boldsymbol{f}\ (\boldsymbol{x}\ , \boldsymbol{y}, \boldsymbol{z})$ en lugar de $\boldsymbol{f}\ (\langle\ \mathbf{x}, \mathbf{y}, \mathbf{z}\rangle)$.

En general, la función de la que el dominio de definición está compuesto de sucesiones de longitud $\boldsymbol{n}$ y se denomina función de $\boldsymbol{n}$ variables en lugar de $\boldsymbol{f}(\langle \boldsymbol{x_1}\ , \ldots , \boldsymbol{x_n}\rangle)$y se escribe $\boldsymbol{f}\ \boldsymbol{x_1}\ , \ldots \boldsymbol{x_n})$.

Composición de funciones: Estúdiese las propiedades de la composición de funciones. Como composición de funciones se entiende aquí también a la composición de relaciones.

TEOREMA 3.1. Sean $\boldsymbol{f}\ \boldsymbol{y}\ \boldsymbol{g}$ *funciones. Entonces su composición* $\boldsymbol{f} \circ\ \boldsymbol{g}$ *es también una función, tal que*

(1) $\quad \boldsymbol{Dom}\ \boldsymbol{f} \circ\ \boldsymbol{g} = \{\boldsymbol{x} \mid \mathbf{g}\ (\mathbf{x})\ \in \boldsymbol{Dom}\ \boldsymbol{f}\}$;

(2) $\quad (\boldsymbol{f} \circ\ \boldsymbol{g})\ (\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{g}\ (\boldsymbol{x}))$ Para cada $\boldsymbol{x}\ \in \boldsymbol{Dom}(\boldsymbol{f} \circ\ \boldsymbol{g}\ )$;

$(\mathbf{3}) \quad \boldsymbol{f} \circ\ \boldsymbol{g} = \{\langle\ \boldsymbol{x}, \boldsymbol{f}\big(\boldsymbol{g}(\boldsymbol{x})\big)\rangle \mid \boldsymbol{g}(\boldsymbol{x})\ \in \boldsymbol{Dom}\ \ \boldsymbol{f}\}$.

Demostración. Por definición, se deduce que la composición de relaciones binarias $\boldsymbol{f} \circ\ \boldsymbol{g}$ es un conjunto de todas las pares de $\langle \boldsymbol{x}\ , \mathbf{y}, \rangle$,tal que para el conjunto de $\boldsymbol{z}$ se cumplen simultáneamente

$\langle\ \boldsymbol{x}, \boldsymbol{z}\rangle \in \boldsymbol{g}$ y $\langle \boldsymbol{z}, \mathbf{y}\rangle \in \boldsymbol{f}$,por lo tanto

$$\boldsymbol{f} \circ\ \boldsymbol{g} = \{\langle\ \boldsymbol{x}, \boldsymbol{y}\rangle\ \mid \exists \mathbf{z}(\langle \boldsymbol{x}\ , \boldsymbol{z}\rangle\ \in \boldsymbol{g} \wedge \langle\ \boldsymbol{z}, \boldsymbol{y}\rangle\ \in \boldsymbol{f})\}.$$

Como $\boldsymbol{g}$ es una función de $\langle \boldsymbol{x}\ , \boldsymbol{z}\rangle \in \boldsymbol{g}$ significa que $\boldsymbol{x} \in \boldsymbol{Dom}\ \boldsymbol{g}$ y $\boldsymbol{z} = \boldsymbol{g}(\boldsymbol{x})$.Ya que $\boldsymbol{f}$ es una función, la inclusión $\langle \boldsymbol{z}, \mathbf{y}\rangle$ y $\in \boldsymbol{f}$quiere decir que:

$\boldsymbol{z = g(x) \in Domf}$ Y $\boldsymbol{y = f(z) = f\big(g(x)\big)}$,

Por lo tanto:

$\boldsymbol{f \circ g = \{\langle x, y\rangle \mid \langle \mathbf{g}(x), y\rangle \in f\}}$;

$\langle x, y\rangle \in \boldsymbol{f \circ g \leftrightarrow y = f(g) \wedge (g * (x) \in Domf)}$;

$\boldsymbol{f \circ g \{\langle x, f\big(g(x)\big)\rangle \mid \mathbf{g}(x) \in Domf\}}$.

Por lo tanto, $\boldsymbol{f \circ g}$ es una función que satisfacen a las igualdades (1), (2), (3).□

COROLARIO 3.2. Sean $\boldsymbol{f}$ y $\boldsymbol{g}$ función cualquieras; se tiene:

(a) $\boldsymbol{Dom\,(f \circ g) \subset Dom\, g, Im(f \circ g) \subset Im\, f}$;

(b) si $\boldsymbol{Im\, g \subset Dom\, f}$, $\boldsymbol{en}$tonces $\boldsymbol{Dom\,(f \circ g) = Dom\, g}$;

(c) Si $\boldsymbol{Im\, g = Dom\, f}$, $\boldsymbol{entonces\ Dom\,(f \circ g) = Dom\, g}$ y $\boldsymbol{Im\,(f \circ g) = Im\, f}$.

TEOREMA 3.3. Si $\boldsymbol{g}$ es una función del conjunto $\boldsymbol{A}$ en $\boldsymbol{B}$ y $\boldsymbol{f}$ una función del conjunto de $\boldsymbol{B}$ en $\boldsymbol{C}$, entonces $\boldsymbol{f \circ g}$ es una función del conjunto $\boldsymbol{A\ en\ C}$.

DEMOSTRACIÓN. Por hipótesis, $\boldsymbol{Im\, g \subset Dom\, f = B}$.

Según el corolario 3.2, se deduce que:

$\boldsymbol{Dom\, f \circ g = Dom\, g = A}$, $\boldsymbol{Im\, f \circ g \subset Im\, f \subset C}$.

Por lo tanto, $\boldsymbol{f \circ g}$ es una función del conjunto $\boldsymbol{A\ en\ C}$. □

TEOREMA 3.4. Si $\boldsymbol{g}$ es una función del conjunto $\boldsymbol{A\ en\ B}$ y $\boldsymbol{f}$ una función del conjunto $\boldsymbol{B\ en\ C}$,entonces $\boldsymbol{f \circ g}$ es una función del conjunto $\boldsymbol{A\ en\ C}$.

Este TEOREMA se deduce directamente del TEOREMA 3.3 y del corolario 3.2.

TEOREMA 3.5.*La composición de funciones es asociativa, es decir que $\boldsymbol{f \circ (g \circ h) = (f \circ g) \circ h}$ para todas las funciones $\boldsymbol{f}$, $\boldsymbol{g}$ y $\boldsymbol{h}$.*

El TEOREMA 3.5 se deriva directamente del TEOREMA 2.2.

DEFINICIÓN. La función $\boldsymbol{\mathbf{i}_A(x) = x}$ a cada $\boldsymbol{x}$ de $\boldsymbol{A}$ se denomina *función idéntica (o unitaria) del conjunto $\boldsymbol{A}$ en el mismo.*

TEOREMA 3.6. *Sea $\boldsymbol{f}$ la aplicación del conjunto $\boldsymbol{A}$ en $\boldsymbol{B}$. Entonces $\boldsymbol{f \circ f^{\smile} = \mathbf{i}_B}$.*

Demostración. La inversa de $\boldsymbol{f^{\smile}}$ de la función $\boldsymbol{f}$ es una relación binaria, talque

$\boldsymbol{f^{\smile} = \{\langle y, x\rangle \mid \langle x, y\rangle \in f\}}$.

Por definición de la composición de relaciones

(1) $f \circ f^{\smile} = \{\langle y, z\rangle \mid \exists x\ (\langle x, y\rangle) \in f^{\smile} \wedge = \langle x, z\rangle \in f\}$.

De $\langle y, z\rangle \in f^{\smile}$ y $\langle y, z\rangle \in f^{\smile}$, se cumple que

(2) $\langle x, y\rangle \in f$ y $\langle y, z\rangle \in f$.

Como $\boldsymbol{f}$ es una función, de (2) se deduce que la igualdad $\boldsymbol{y = z}$. Por lo tanto (1) se puede escribir de la siguiente forma

$f \circ f^{\smile} = \{\langle y, y\rangle \mid \exists x\ (\langle x, y\rangle \in f)\}$.

Donde, ya que $\boldsymbol{f}$ es la aplicación de $A\ en\ B$,

$f \circ f^{\smile} = \{\langle y, y\rangle \mid y \in B\}$.

Por lo tanto, $f \circ f^{\smile} = \mathrm{i}_B$.□

TEOREMA 3.7. *Sean f, g, h las funciones que satisfacen a la condición*

(1) $Dom\, g = Dom\, h \subset Im\, f$.

Entonces, si $g \circ f = h \circ f$, se tiene que $g = h$.

Demostración. Supóngase que

(2) $g \circ f = h \circ f$.

En virtud de (1) para todo y de $Dom\ g$ se encontrara un elemento de x, tal que $y = f(x)$. De donde, en virtud de (2), se deduce que $g(y) = g\big(f(x)\big) = h(f(x)) = h(y)$, es decir que $g(y) = h(y)$ para toda y de $Dom\ g$. Además, en virtud de que (1) $Dom\ g\ = Dom\ h$. Por lo tanto $g = h$. □

Funciones inyectivas. Entre las funciones estudiadas en las matemáticas, las inyectivas juegan un papel muy importante.

DEFINICIÓN. La función f es *inyectiva* si para todos los elementos de x, y (extraídos del $Dom\ f$) se deduce de la condición $f\ (x) = f(y)$ y que $x = y$.

En otros términos, la función f es inyectiva si para todos los elementos de x, y, z puesto que $\langle\ x, z\rangle\ \in f$ y $\langle y, z\rangle\ \in f$ se deduce que $x = y$.

En virtud de la ley de contra reciproco, de la definición se deduce que la *función f es inyectiva si y solo si para todo elementos cualesquiera de x* ,y, la función de f ocupa valores distintos *en los casos en donde* $x\ \neq y, f(x) \neq f(y)$, dicho de otro modo, para todos los argumentos distintos.

DEFINICIÓN. Se denomina *permutación o transformación del conjunto A* a una función inyectiva de un conjunto no vacío A en el mismo.

En particular, una función idéntica o unitaria $\mathbf{i_A}$ del conjunto A en el mismo es una permutación, es decir, que una función semejante a $\mathrm{i}_\mathrm{A}\ (x) = x$ para cada $x\ de\ A$.

PROPOSICIÓN 3.8. *Si f es una función del conjunto A en el conjunto B, se tiene que* $f \circ\ \mathrm{i}_A = f,\ \mathrm{i}_B\ \circ f = f$. □

TEOREMA 3.9. *Se denomina función inyectiva, a la composición de dos funciones inyectivas cualesquiera.*

DEMOSTRACIÓN. Sean $f\ y\ g$ funciones inyectivas.

Conforme a la función inyectiva f para todos los conjunto de x, y, si $f\big(g(x)\big) = f\big(g(y)\big)$, se tiene que $g(x) = g(y)$. Además, en virtud de la función inyectiva g para todo x, y, aun cuando $g(x) = g(y)$, se tiene que $x = y$. Por lo tanto, para x, y cualesquiera, si $f\big(g(x)\big) = f\big(g(y)\big)$, se tiene que $x = y$. Por lo tanto, para todas x, y aun cuando $(f \circ g)(x) = (f \circ g)(y)$, se tiene que $x = y$.

La función $f \circ g$ es inyectiva. □

COROLARIO 3.10. *Una composición de dos permutaciones cualesquiera del conjunto A es una permutación del conjunto A.*

Este corolario se deriva directamente de los TEOREMAs 3.4 y 3.9.

Sea f una función. La inversa de $f^{\smile}\ = \{\langle\ x, y\rangle\ |\langle\ y, x\rangle\ \in\ f\}$ de la función f puede no ser una función. Así por ejemplo, si se dada una función $f = \{\langle x, x^2\ \rangle\ |\ \ x \in Z\}$, donde $\boldsymbol{Z}$ es el conjunto de todos los enteros, la relación $f^{\smile}\ = \{\langle x^2\ , x\rangle\ | \in \boldsymbol{Z}\}$ no es una función, puesto que no posee pares de $\langle\ 1,\ 1\rangle$ y $\langle\ 1, -1\rangle$ de primeros elementos iguales y segundos elementos distintos.

Sin embargo para una función $g = \big\{\langle x\ , 2x\rangle\ |\ \in \boldsymbol{N}\big\}$, donde $\boldsymbol{N}$ es el conjunto de todos los enteros no negativos, la Inversa $g^{\smile}\ = \big\{\langle 2x\ , x\rangle\ |x\ \} \in \boldsymbol{N}\big\}$ es una función.

PROPOCICIÓN 3.11. *Si $f\ y\ g$ son funciones, se tiene:*

(a) $Dom\, f^{\smile} = Im\, f$; (c) $(f^{\smile})^{\smile} = f$;
(b) $Im f^{\smile} = Dom\, f$; (d) $(f \circ g)^{\smile} = g^{\smile} \circ f^{\smile}$.

Esta proposición se deduce directamente de la proposición 2.1. y del TEOREMA 2.3.

COROLARIO 3.12. *Si f es una función del conjunto A en B y $f^{\smile}$ una función, $f^{\smile}$ es una función del conjunto B en A.*

TEOREMA 3.13. *La inversa $f^{\smile}$ de la función f es una función si y solo si la función f es inyectiva.*

DEMOSTRACIÓN. La relación $f^{\smile}$ es una función si y solo si para todas x, y, z se tiene que $x = y$ en el caso donde $\langle z, x\rangle \in f^{\smile}$ y $\langle z, y\rangle \in f^{\smile}$. Esta condición es equivalente a la condición que indica que la función f es inyectiva:

para todas x, y, z si $\langle x, z\rangle \in f$ y $\langle y, z\rangle \in f$, se tiene $x = y$. Por lo tanto, la relación $f^{\smile}$ es una función si y solo si la función f es inyectiva. □

COROLARIO 3.14. *Si f es una función inyectiva, $f^{\smile}$ también lo es. Además, si f es una función inyectiva de A en B, entonces $f^{\smile}$ es una función inyectiva de B en A.*

TEOREMA 3.15. Sean f, g, h funciones que satisfacen a las condiciones:

(1) $f \circ g = f \circ h$;
(2) $Dom\, g = Dom\, h$, $Im\, g \subset Dom\, f$, $Im\, h \subset Dom\, f$.

En este caso si la función f es inyectiva, se tiene $g = h$.

Demostración. Supóngase que la función f es inyectiva.
En virtud de las condiciones (1) y (2), se tiene
$f(g(x)) = f(h(x))$ para todo x de $Dom\, g$.
Debido a la función inyectiva f se tiene $g(x) = h(x)$ para todo x de $Dom\, g$. Además según la condición (2) de $Dom\, g = Dom\, h$. Por lo tanto, $g = h$. □

Funciones inversa. Sea f la función del conjunto A en B.

DEFINICIÓN. La función φ se denomina *inversa a la izquierda* de la función f si φ es la función de B en A y si $\varphi \circ f = \mathfrak{i}_A$. La función que posea una inversa a la izquierda se denomina *inversible a la izquierda*.

DEFINICIÓN. La función h se denomina *inversa a la derecha* de la función f si h es la función de B en A y si $f \circ h = \mathfrak{i}_B$. A la función que posee una inversa a la derecha se le denomina *inversible a la derecha.*

DEFINICIÓN. La función g se denomina *inversa* de la función f si g es la función de B en A, $f \circ g = \mathfrak{i}_A$ y $f \circ g = \mathfrak{i}_B$. Se denomina *inversible* a la función que posee una inversa. La función inversa de la función f se designa por el símbolo f^{-1}.

De estas DEFINICIÓNes se deriva: a) si φ es la función inversa a la izquierda de f, entonces la función f es la inversa a la derecha de φ; b) si h es la función inversa a la derecha de f, entonces la función f es la inversa a la izquierda de h; c) si la función g es la inversa de f, entonces la función f, es la inversa de g; en este caso las funciones f y g Se denominan *mutuamente inversas.*

TEOREMA 3.16. *Si f es la función inyectiva del conjunto A en B, entonces se tiene $f^{\smile} \circ f = \mathfrak{i}_A$, $f \circ f^{\smile} = \mathfrak{i}_B$.*

Demostración. Sea f la función inyectiva del conjunto A en B. Entonces, según el TEOREMA 3.13, la relación $f^{\smile}$ también es una función, para todos x, y la condición

(1) $f^{\smile}(y) = x$

al considerar el equivalente

(2) $f(x) = y$.

En virtud de (2) y (1) para todo $x\ de\ A$, se cumple que:

$f^{\smile}\ \big(f(x)\big) = x$ y $(f^{\smile}\ \circ f\ )(x) = x$,

sea $f^{\smile}\ \circ f = \mathrm{i}_{\mathrm{A}}$. Además, conforme a (1) y (2) para toda $y\ de\ B$, se tiene:

$f\big(f^{\smile}\ (y)\big) = y$ Y $(f \circ f^{\smile}\ )(y) = y$,

Sea $f \circ f^{\smile}\ = \mathrm{i}_{\mathrm{B}}$ □

COROLARIO 3.17. *Si f es una función inyectiva del conjunto $A\ en\ B$, f es una función inversible, la función $f^{\smile}$ es la inversa de f.*

COROLARIO 3.18. *Si f es una permutación del conjunto A, $f^{\smile}\ \circ f = \mathrm{i}_{A}$ y $f \circ f^{\smile}\ = \mathrm{i}_{A}$.*

TEOREMA 3.19. *Sea f una funcion del conjunto $A\ en\ B$ inversible a la izquierda. Toda función inversa a la izquierda de f coincide con $f^{\smile}$ y es igualmente una inversa a la derecha de f que es inversible.*

Demostración. Sea $\varphi\colon B \to A$ es una función inversa a la izquierda de $\boldsymbol{f}$, quieredecir,

(1) $\varphi \circ f = \mathrm{i}_{\mathrm{A}}$.

Posterior al TEOREMA 3.6 y la proposición 3.8, se cumple que:

(2) $f \circ f^{\smile}\ = \mathrm{i}_{\mathrm{B},}\qquad \mathrm{i}_{\mathrm{A}}\ \circ f^{\smile}\ = f^{\smile}\ ,\qquad \varphi \circ\ \mathrm{i}_{\mathrm{B},} = \varphi.$

En virtud de (2) y (1)

$\varphi = \varphi \circ\ \mathrm{i}_{\mathrm{B},} = \varphi \circ (f\ \circ f^{\smile}\ ) = (\varphi \circ f) \circ f^{\smile}\ = \mathrm{i}_{\mathrm{A}}\ \circ f^{\smile}\ = f^{\smile}\ ,$

por lo tanto, $\varphi = f^{\smile}$. Además, $f \circ\ \varphi = f\ \circ f^{\smile}\ = \mathrm{i}_{\mathrm{B},}$ la función φ es semejante a una inversa a la derecha de f y, por consiguiente, f es inversible. □

TEOREMA 3.20. *Sea f la función del conjunto $A\ en\ B$ inversible a la derecha .Toda función inversa a la derecha de f coincide con $f^{\smile}$ y es semejante a una inversa a la izquierda de f que es inversible.*

Demostración. Sea $h\colon B \to A$ la función inversa a la derecha de f , es decir:

(1) $f\ \circ h = \mathrm{i}_{\mathrm{B},}$.

Seguido del TEOREMA 3.6 y la proposición 3.8, se tiene:

(2) $h \circ h^{\smile}\ = \mathrm{i}_{\mathrm{A}},\qquad \mathrm{i}_{\mathrm{B},} \circ h^{\smile}\ = h^{\smile}\ .$

En virtud de (2) y (1), se cumple que:

$f = f\ \circ \mathrm{i}_{\mathrm{A}} = f\ \circ (h \circ h^{\smile}\ ) = (f \circ h) \circ h^{\smile}\ = \mathrm{i}_{\mathrm{B},} \circ h^{\smile}\ = h^{\smile}\ .$

Según el TEOREMA 2.1. De $f = h^{\smile}$ se deduce que $h = f^{\smile}$ .Ademas, $h \circ f = f^{\smile}\ \circ f = \mathrm{i}_{\mathrm{A}}$,es decir que la función h es semejante a una inversa a la izquierda de f y, por lo tanto, f es inversible. □

TEOREMA 3.21. Las siguientes propiedades de la función f son equipotentes:

(a) La inversa $f^{\smile}$ de la función f es una función;
(b) La función f es inyectiva;
(c) La función f es inversible a la derecha;
(d) La función f es inversible a la izquierda;
(e) La función f es inversible;
(f) Todas las funciones inversas de f (a la izquierda, a la derecha, a ambos lados) existen y coinciden con $f^{\smile}$.

Demostración. Según el TEOREMA 3.13, las propiedades (a) y (b) son equipotentes.

Si f es una función inyectiva de $A\ en\ B$, entonces según el TEOREMA 3.14 $f^{\smile}$ es una función de $B\ en\ A$ y $f \circ f^{\smile}\ = \mathrm{i}_{\mathrm{B},}$,La función f es inversible a la derecha. Por lo tanto, de (b) se deduce (c).

Si la función f es inversible a la derecha, entonces, según el TEOREMA 3.20, esta es igualmente inversible a la izquierda. Por lo tanto, de (c) se deduce (d).

Si la función f es inversible a la izquierda, entonces en virtud del TEOREMA 3.19, la función f es inversible. Por lo tanto, de (d) se deriva (e).

Supóngase que la función f es inversible, Entonces esta es inversible a la izquierda y a la derecha. Según los TEOREMAs 3.19 Y 3.20, todas las funciones inversas de f coinciden con $f^{\smile}$.

Si la condición (g) se cumple, la inversa de $f^{\smile}$ de la función f es una función. Por lo tanto de (g) se deduce (a).

Por lo tanto, las propiedades (a), (b), (c), (d), (e), (g) son equipotentes. □

TEOREMA 3.22. Si las funciones f y g son inversible las funciones $f \circ g$ igualmente lo es y $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Demostración. Sean f y g funciones inversible. Entonces, sus inversas $f^{\smile}$ y $g^{\smile}$ son funciones y

(1) $f^{\smile} = f^{-1}$, $g^{\smile} = g^{-1}$.

Según el TEOREMA 2.3, se cumple:

(2) $(f \circ g)^{\smile} = g^{\smile} \circ f^{\smile}$.

Como $g^{\smile}$ y $f^{\smile}$ son funciones, su composición $g^{\smile} \circ f^{\smile}$ es una función; por lo tanto, en virtud de (2), $(f \circ g)^{\smile}$ es una función. Por tanto la función $f \circ g$ es inversible y se tiene:

(3) $(f \circ g)^{\smile} = (f \circ g)^{-1}$.

En la base de las igualdades (1), (2), (3) se concluye que la función $f \circ g$ es inversible y $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. □

Restricción de una función. Un caso particular de restricción de una relación binaria es la restricción de una función.

DEFINICIÓN. La función g se denomina *restricción (o striction) de la función f* si $g \subset f$. Si $g \subset f$ se dice igualmente que f es la *extensión (prolongación) de la función g*.

DEFINICIÓN. La función g se le denomina *restricción de la función f por el conjunto A (o striction de la función f al conjunto A)* si $g \subset f$ y si $Dom\ g = A$.

La restricción de la función f el en conjunto A se denota $f_{A,}$ O f | A.

PROPOSICION 3.23. Si $A \subset Dom\ f$, la función $f \circ i_{A,}$ es entonces una restricción de la función f en el conjunto A, es decir, $f_{A,} = f \circ i_A$.

Esta proposición se deriva directamente de la definición de la función f_A.

TEOREMA 3.24. La función g es una restricción de la función f si y solo si $Dom\ g \subset Dom\ f$ y $g(x) = f(x)$ para toda x extraida de $Dom\ g$.

Demostración. Supóngase que $g \subset f$. Entonces, $Dom\ g \subset Dom\ f$ y para toda $x \in Dom\ g$ de $\langle x, y \rangle \in g$ se deduce que $\langle x, y \rangle, \in f$ y, por lo tanto, $g(x) = f(x)$.

Admítase ahora que $Dom\ g \subset Dom\ f$ y $g(x) = f(x)$ para todos $x \in Dom\ g$. Entonces, para todos x, y de $\langle x, y \rangle, \in g, es$ decir, de $y = g(x)$,se deduce que $y = f(x)$ y $\langle x, y \rangle \in f$, por lo tanto, $g \subset f$. □

Ejercicios

1. ¿Cuáles son funciones entre las siguientes relaciones? Indicar sus dominios de definición y sus dominios de valores:

(a) $\{\langle x, y \rangle \mid x, y, \in N$ y $, y = x^2\}$;

(b) $\{\langle x, y \rangle \mid x, y, \in N$ y $x < y \leq x + 1\}$;

(c) $\{\langle x, y \rangle \mid x, y, \in Z$ y $y = x^2\}$;

(d) $\{\langle x, y \rangle \mid x, y, \in N$ x divide a $y\}$;

(e) $\{\langle x, y \rangle \mid x, y, \in Z$ y $y = |x|\}$;

(f) $\{\langle x, y \rangle \mid x, y, \in Z$ y $y = y^2\}$.

Aquí y más allá de Z es el conjunto de todos los entero y N el conjunto de todos los enteros no negativos.

2. Sea $A = \{0,1\}$un conjunto de dos elementos. Investigar todas las funciones del conjunto A en el mismo e indicar las inyectivas.
3. Investigar todas las funciones del conjunto $A = \{0,1,2,\}$en el conjunto $B = \{0,1\}$.
4. Demostrar que para cada función f y un conjunto cualquiera $Af(A) = \emptyset$ si y solo si $A \cap Dom\ f = \emptyset$.
5. Demostrar que si f es una función del conjunto $A\ en\ A$ tal que $f \circ f = f$,y se tiene $f = \mathrm{i}_A$.
6. Demostrar que si f es una función y A y B conjuntos, entonces $f(A \cap B) \subset f(A)\ \cap f(B)$. Demostrar por medio de ejemplos que las igualdades $f(A \cap B) = f(A) \cap f(B)$ puede no tener lugar.
7. Sea $R \subset A$ X B. Demostrar que R es la función del conjunto $A\ en\ B$ si y solo si $R \circ R^{\smile}\ \subset \mathrm{i}_B$ y $\mathrm{i}_A\ \subset R^{\smile}\ \circ R$.
8. Demostrar que cada una de las siguientes funciones posee una inversa.
Buscar el dominio de definición de la función inversa:
(a) $f = \{\langle x,y\rangle \mid x,y, \in N \quad \text{y} \quad y = 2x + 1\}$;
(b) $f = \{\langle\ n,\ n^2\ \rangle \mid n \in N\}$;
(c) $f = \{\langle x,y\rangle \mid x,y, \in N\ \text{y}\ y =\ x^2\ \}$.
9. Para todos los conjuntos A, B y C demostrar que existe:

(a) Una función inyectiva del conjunto $A\ X\ B$ en $B\ X\ A$;

(b) Una función inyectiva del conjunto $(A \text{ X } B) \text{ X } C$ en $A \text{ X } (B \text{ X } C)$.

10. Sea f una función del conjunto A en A.Demostrar que si $f \circ f \circ f = \mathrm{i}_A$, y que f es una función inyectiva del conjunto A en A.

11. Sea f una función del conjunto A en B.Demostrar que si $C, D \subset B\ \text{Y} \cap D = \emptyset$, entonces $f^{\smile}\ (A) \cap f^{\smile}\ (B = \emptyset$.

12. Demostrar que para toda función f se satisfacen las relaciones:

(a) $f^{\smile}\ (A\ \cup B) = f^{\smile}\ (A) \cup f^{\smile}\ (B)$;

(b) $f^{\smile}\ (A) \cap B) = f^{\smile}\ (A) \cap f^{\smile}\ (B)$;

(c) $f^{\smile}\ (A \setminus B) = f^{\smile}\ (A) \setminus f^{\smile}\ (B)$;

(d) $A \subset B \rightarrow f^{\smile}\ (A) \subset f^{\smile}\ (B)$.

13. Demostrar que sí $A \subset Dom\ f$ y $B \subset Im\ f$,entonces se tiene

(a) $A \subset f^{\smile}\ \big(f(A)\big)$; $(b)\ \ f\big(f^{\smile}\ (B)\big) = B$.

14. Demostrar que $f(A) \setminus f(B) \subset f(A \setminus A)$ para cada función de f y todos los conjuntos A y B. Si f es una función inyectiva, se tiene $f(A) \setminus f(B) = f(A \setminus B)$ para todos los conjuntos A y B.

15. Sea f una función del conjunto A en B y g una función del conjunto B en C.Demostrar que:

(a) Si La función g $\circ f$ es inyectiva, y que si f también lo es; (b) Si g $\circ f$es una función de A en C, g es una función de B en C.

16. Demostrar que la función f: $A \rightarrow B$ es una funcion inyectiva del conjunto A en B si y solo si existe una función g: $B \rightarrow A$ Tal que g $\circ f = \mathrm{i}_A$ y g $\circ f = \mathrm{i}_B$.

17. Demostrar que la relación binaria $A \subset A$ XB es una función inyectiva del conjunto A en Bsi y solo si

$$R \circ R^{\smile}\ = \mathrm{i}_B\ y\ R^{\smile}\ \circ\ R = \mathrm{i}_A\ .$$

18. Demostrar que la función f satisface a la condición $f(A \cap B) = f(A) \cap f(B)$para todos los conjuntos de A y B si y solo si la función f es inyectiva.

19. Sean A y B conjuntos finitos compuestos de m y n elementos respectivamente, con $m \leq n$. Demostrar que existe $n(n-1)\ldots(n-m+1)$funciones inyectivas del conjunto A en B.

20. Sean A y B conjuntos finitos compuestos de m y n elementos respectivamente.

(a) ¿Para cuales $m\ y\ n$ existen funciones inyectivas del conjunto A en B ?

(b) ¿Cuantas funciones hay del conjunto A en B?

(c) ¿Cuantas relaciones binarias se necesitan entre los elementos del conjunto A y B?

§ 4. Relación de equivalencia

Algunos tipos de relaciones binarias. De acuerdo con algunas propiedades importantes las relaciones binarias se dividen en tipos:

DEFINICIÓN. La relación binaria R en el conjunto A es *reflexiva* en el conjunto A si para cada x de A, se tiene xRx.

La relación es reflexiva en A si y solo si $\mathfrak{i}_A \subset R$, donde $\mathfrak{i}_A = \{\langle x, x\rangle \mid x \in A\}$. Si la relación R es reflexiva, entonces cada vértice de su grafo está cerrada. De lo contrario, un grafo cuyo vértice tiene una curva cerrada representa una cierta relación reflexiva.

A modo de ejemplos de relaciones reflexivas se puede indicar la relación de paralelismo en un conjunto de direcciones del plano, la relación de igualdad en un conjunto cualquiera de números y la relación de divisibilidad en un conjunto cualquiera de enteros.

DEFINICIÓN. La relación binaria R en el conjunto A es *anti reflexiva* en A si para cada x de A $\langle x, x\rangle \notin R$, es decir si para cada x de A la condición xRx no se cumple.

La relación R es anti reflexiva en A si y solo si $\mathfrak{i}_A \cap R = \emptyset$. Si la relación R es anti reflexiva, ningún vértice de su grafo está cerrado. Recíprocamente, si ningún vértice del grafo posee una curva cerrada, entonces el grafo representa una relación anti reflexiva.

Por ejemplo, son anti reflexivas aquellas relaciones de desigualdad ($\neq$) en un conjunto cualquiera de números y la relación de perpendicularidad en un conjunto de rectas de un plano.

DEFINICIÓN. La relación binaria R (en A) se denomina *transitiva* (en A) si para cualquier x, y, z del dominio de la relación R (en A) de xRy y yRz.

La relación R es transitiva si y solo si $R \circ R \subset R$. Si la relación R es transitiva, su grafo, para cada pareja de líneas será $\langle x, y\rangle$ y $\langle y, z\rangle$, que posee una línea de clausura $\langle x, z\rangle$ y recíprocamente.

Por ejemplo, la relación de divisibilidad en un conjunto de enteros es transitiva. La relación de desigualdad ($\neq$)no es transitiva.

DEFINICIÓN. Una relación binaria R (en A) se denomina *simétrica* (en A) si para cualquiera x, y de dominio de la relación R (de A) se deducen xRy y yRx.

La relación R es simétrica si y solo si $R^{\smile} = R$. Si la relación R es simétrica, cada línea de su grafo no está orientada. Recíprocamente: un grafo de líneas no orientadas representa una cierta relación binaria simétrica.

Por ejemplo, son simétricas todas aquellas relaciones de paralelismos de rectas, la relación de perpendicularidad de rectas y la relación de igualdad.

DEFINICIÓN. Una Relación binaria R (sobre A) se denomina *anti simétrica* (en A) sí para toda $x,\ y$ cualquier dominio de la relación R (de A) de xRy y yRx se deduce que $x = y$.

La relación R es anti simétrica en (sobre) A si y solo si $R \cap R^{\smile} \subset \mathfrak{i}_A$. El grafo de la relación anti simétrica no tiene líneas no orientadas, pero puede que tenga curvas cerradas.

Por ejemplo, la relación de inclusión $\subset$ en una colección cualquiera de conjuntos es anti simétrica.

DEFINICIÓN. Una relación binaria R en un conjunto A se denomina *asociada* en A si para todos los elementos de x, y del conjunto A de $x \neq y$ se deduce que $xRy \vee yRx$.

Una relación R está asociada con A si y solo si $A \times A \setminus \mathfrak{i}_A \subset R \cup R^{\smile}$.

Una relación binaria R en A está asociada en A si y solo si para todas x, y de A se tiene ya sea $x = y, xRy$ o yRx, es decir que $A \times A = \mathfrak{i}_A \subset R \cup R^{\smile}$.

El grafo de una relación asociada está dotado de las siguientes propiedades: dos vértices cualesquiera (diferentes) de un grafo están unidos por una línea. La reciproca es igualmente verdadero.

Es así por ejemplo, que la relación común $\ll$ inferior a $\gg$ ($<$) en una colección cualquiera de números es una relación asociada.

Relación de equivalencia. Una de las relaciones más importantes de la relación binaria es la relación de equivalencia.

DEFINICIÓN. La relación binaria en el conjunto A se denomina *relación de equivalencia en* A si esta es reflexiva, simétrica o transitiva (sobre A).

Con frecuencia la relación de equivalencia se designa por los símbolos $\sim, \approx\ o\ \equiv$.

Ejemplos. 1. Sean A un conjunto no vacio y $\mathfrak{i}_A = \{\langle x, x\rangle \mid x \in A\}$ una relación de identidades el conjunto A. La relación $\mathfrak{i}_A$ es la relación de equivalencia en A.

2. Sean A un conjunto de rectas de un plano y $R = \{\langle x,\ y\rangle \mid x, y \in A$ y x es paralela en $y\}$ la relación de paralelismo. Por lo tanto, la relación de paralelismo en A es una relación de equivalencia.

3. Sea Z el conjunto de todos los enteros y m un número entero distinto de cero. Por lo tanto la relación

$R = \{\langle x,\ y\rangle \mid x, y \in Z$ y $x - y$ divisible por $m\}$

a esta relación se le denomina como *congruencia módulo* m. Esta es una relación de equivalencia en Z.

4. Sea A un conjunto de segmentos orientados de un plano dado.

La relación de equivalencia de los segmentos orientados es una relación de equivalencia en A.

5. La relación de semejanza en un conjunto de triángulos de un plano dado es una relación de equivalencia.

6. Dos conjuntos se denominan *equiponentes* si existe una función inyectiva de un conjunto a otro. La relación de equipotencia en cualquier colección dada de conjuntos es una relación de equivalencia.

DEFINICIÓN. Sean R una relación de equivalencia en A y $a \in A$.

Se denomina clase *de equivalencia generada por el elemento* a al conjunto $\{\in A \mid xRa\}$, es decir un conjunto x de A para la cual $\langle x,\ a\rangle \in R$.

La clase de equivalencia generada por el elemento a se denota a/R o $[a]_{R.}$ La colección de todas las clases de equivalencia de la relacion R en el conjunto A se denota A/R o $[A]_{R.}$

DEFINICIÓN. Todo elemento de la clase de equivalencia se denomina al representar esta clase. Se define *sistemas completos de representantes de estas clases de equivalencia* al conjunto de representantes de todas las clases, uno por clase.

En el ejemplo 1 las clases de equivalencia se constituyen por subconjuntos A en un elemento. En el ejemplo 2 las clases de equivalencia tienen el nombre de *haces de rectas paralelas.* En el ejemplo 3 las clases de equivalencias se denominan *clases residuales módulo* m, cada clase se compone de todos los números que luego de dividirlos por m dan como resultado un mismo residuo. En el ejemplo 4 las clases de equivalencia están constituidas por *vectores* de un plano. En el ejemplo 5 las clases de equivalencia son conjuntos de triángulos semejantes dos a dos. En el ejemplo 6 las clases de equivalencia son clases de conjuntos equivalentes.

Conjunto cociente. Sea A un conjunto no vacio.

DEFINICIÓN. Se Denomina *conjunto cociente del conjunto* A *por la equivalencia* R en el conjunto A/R de todas las clases de equivalencia.

DEFINICIÓN. Se define *partición de un conjunto* A a una familia de subconjuntos no vacios para la cual cada elemento de A es estrictamente incluido en un mismo término de la familia.

Por lo tanto, la partición del conjunto A es una familia de sus subconjuntos no vacios de la que la reunión coincide con A mientras que la intersección de dos cuales quiera de sus subconjuntos es vacio.

TEOREMA 4.1. *Sea* R *una relacion de equivalencia en un conjunto* A *(no vacío). Entonces el conjunto cociente* A/R *es una partición del conjunto* A.

Demostración. Cada elemento a del conjunto A pertenece a la clase de equivalencia a/R . Se debe demostrar que cada elemento de A pertenece estrictamente a un término de la familia A/R . Por eso basta demostrar que las clases de equivalencia que posean al menos un elemento común coinciden. Sean a/R y b/R las clases de equivalencia en un elemento común c, x que tiene un elemento a/R , entonces se tiene que xRa , $a\,Rc$, aRb y en virtud de la transitividad de a relación $R\,xRb$. Es así como, $a/R \subset b/R$. De manera análoga muéstrese que $b/R \subset a/R$. Entonces se tiene que $a/R = b/R$. Como resultado, se establece que el conjunto cociente A/R es una partición del conjunto A .□

COROLARIO 4.2. *Sea* R *una relación de equivalencia sobre el conjunto* A *, por lo tanto:*

(1) $a \in a/R$ *para toda* a *de* A .
(2) *para todos* a, b *de* A $a/R = b/R$ *si y solo si* aRb;
(3) $a/R \neq b/R$ *si y solos si* $a/R \cap b/R = \emptyset$;
(4) $A = \bigcup_{x \in A} x/R$.

Este corolario se deriva directamente del TEOREMA 4.1.

Sean S una partición del conjunto no vacio A y R_S una relación binaria definida de la siguiente manera: $\langle x, y\rangle \in R_S$ si y solo si x y y pertenecen al mismo término de la familia S.

TEOREMA 4.3. *La relación* R_S *asociada a la partición S de un conjunto no vacio* A *es una relación de equivalencia en* A *, además, el conjunto cociente* $A/\ R_S$ *coincide con la partición* S.

La demostración del TEOREMA se efectúa fácilmente y se deja a opción del lector el bosquejo a manera de ejercicios.

Equivalencia de función. Sea f la función del conjunto A en B. Considérese una relacion binaria R sobre A tal que xRy solo tenga lugar si y solo si $f(x) = f(y)$.

DEFINICIÓN: Sea f una función del conjunto A en B. La relacion binaria R.

$R = \{\langle x, y\rangle \mid f(x) = f(y), \quad x, y \in A\}$,

Se denomina *equivalencia de función* f.

TEOREMA 4.4. Sean f una función cualquiera y $A = Dom\, f$. *La relación de equivalencia de la función* f *es una relación de equivalencia sobre el conjunto* A.

Demostración. Sea R una equivalencia de una función f. La relacion R es reflexiva sobre A, puesto que $f(x) = f(x)$ para toda x de A. La relación R es transitiva, puesto que para todas x, y, z se deducen de $f(x) = f(y)$ y $f(y) = f(z)$ que es igual a $f(x) = f(z)$. La relación R es simétrica puesto que para todo x, y de $f(x) = f(y)$ se deducen $f(y) = f(x)$. Por consecuencia, R es una relación de equivalencia sobre el conjunto A. □

Si $a \in A = Domf, f(a) = b$ y R es una equivalencia de función $\boldsymbol{f}$, la clase de equivalencia generada por el elemento a es $f^{\smile}(b)$. El conjunto $\{f^{\smile}(x) \mid x \in Im\, f\}$ es el conjunto cociente del conjunto A relativamente en la equivalencia R, es decir $A/R = \{f^{\smile}(x) \mid x \in Im\, f\}$.

Toda relación de equivalencia R_1 sobre un conjunto A se puede asociar a una relación de equivalencia de una cierta función del conjunto A. De hecho, se puede definir a la función natural del conjunto A sobre el conjunto cociente A/R_1 asociando a cada x de A la clase de equivalencia única xA/R_1 que contiene a cada x. Se verifica fácilmente que la relación de equivalencia R_1 coincide con la equivalencia de función natural del conjunto A sobre A/R_1.

Ejercicios

1. Estudiar las siguientes relaciones desde las perspectivas de la re flexibilidad, de la no re flexibilidad, de la simetría, de la anti simetría, de la transitividad:

(a) $\{\langle x, y\rangle \mid x, y \in Z$ y $x \leq y + 1\}$, donde Z es el conjunto de todos los enteros;

(b) $\{\langle x, y\rangle \mid x, y \in Z$ y $x^2 = y^2\}$;

(c) $\{\langle x, y\rangle \mid x, y \in Z$ y $|x| = |y|\}$;

(d) {X, Y| X, Y ⊂ Z y X ∩ Y = ∅};

(e) $\{\langle x, y\rangle \mid x, y \in N$ y divide y} (N es el conjunto de todos los enteros no negativos);

(f) $\{\langle x, y\rangle \mid x, y \in N$ y $x < y\}$;

(g) $\{\langle x, y\rangle \mid x, y \in N$ y $x+y = 1\}$;

(h) $\{\langle x, y\rangle \mid x, y \in N$ y $x \leq y\}$;

(i) $\{\langle x, y\rangle \mid x, y \in N$ y $x \neq y\}$;

(j) $\{\langle x, y\rangle \mid x, y \in Z$ y $x^2 + x = y^2 + y\}$;

(k) $\{\langle x, y\rangle \mid x, y \in Z$ y $x^2 + y^2 = 1\}$;

2. Dar ejemplos de relaciones binarias:

(a) Reflexivas y transitivas pero no anti simétricas;

(b) Transitivas y simétrica pero no reflexivas;

(c) Reflexivas y transitivas pero no simétrica;

(d) Reflexivas y simétricas pero no transitivas.

3. Sea R ⊂ A × A. Demostrar que:

(a) R es reflexiva en el conjunto A si y solo si $i_A \subset$ R;

(b) R es simétrica si y solo si $R^{-1} \subset \mathrm{R}$

(c) R es transitiva si y solo si R $\subset$ R

4. Demostrar que una relación binaria R simétrica y anti simétrica es transitiva.

5. Encontrar todos los conjuntos cociente del conjunto $\{1,2,3\}$.

6. Mostrar que el conjunto $\{1,2,3,4\}$ posea 15 conjuntos cocientes diferentes.

7. Demostrar que si R es una relación binaria transitiva y simétrica en el conjunto A donde A es el dominio de la relación R, R es un equivalente para A.

8. Demostrar que la relación binaria R, cuyo dominio de definición en Dom R= A, es una relación de equivalencia para A si y solo si R R$\subset$ R y $R^{-1} = \mathrm{R}$.

9. Demostrar que si R es una relación de equivalencia para el conjunto A, R es también una relación de equivalencia para A.

10. Demostrar que una intersección de toda colección de relaciones de equivalencia para el conjunto A es una relación de equivalencia para el conjunto A.

11. Demostrar que por todo el conjunto M no vacío existe una función inyectiva del conjunto de todas las particiones del conjunto M del conjunto de todas las relaciones de equivalencia de M.

12. Demostrar que el conjunto cociente Z/ m del conjunto de los enteros Z siguiendo la congruencia módulo m contiene exactamente m elementos.

§5. Relaciones de orden

Relaciones de orden. Sea R una relación binaria en el conjunto A.

DEFINICIÓN. Una relación binaria R en el conjunto A se denomina *relación de orden en el conjunto A u orden en A*, si A es transitiva y anti simétrica.

DEFINICIÓN. Una relación de orden R en el conjunto A se denomina *no estricto*, si es esta es reflexiva en A, es decir, si $\langle x,x\rangle \in R$ para todo x de A.

La relación de orden R se denomina *estricta* (sobre A) si ella es anti reflexiva en A, es decir, si $\langle x,x\rangle \notin R$ para todo x de A. Ahora bien, como la relación transitiva R es anti reflexiva es igualmente anti simétrica, por tanto se puede avanzar en la definición siguiente de equivalente.

DEFINICIÓN. Una relación binaria R en el conjunto A se denomina *orden estricto en A* si es transitiva y no reflexiva en A.

EJEMPLOS. 1. Sea $P(M)$ el conjunto de todo el sub- conjuntos del conjunto M. La relación de inclusión $\subset$ en el conjunto $P(M)$ es una relación de orden no estricta.

2. Las relaciones $< y \leq$ en el conjunto de los números reales son respectivamente de las relaciones de orden estricta y no estricta.

3. La relación de divisibilidad en el conjunto de números naturales es una relación de orden no estricta.

DEFINICIÓN. Una relación binaria R en un conjunto A se denomina *relación de pre orden o pre orden en A* si es reflexiva en A y transitiva.

EJEMPLOS. 1. La relación de divisibilidad en un conjunto de números enteros no es un orden. Ahora bien, ella es reflexiva y transitiva es así un pre orden.

2. La relación $\vDash$ de deducción lógica es una relación de pre orden en el conjunto de las fórmulas de la lógica de aserciones.

Orden total. Un caso particular importante de la relación de orden es el orden total.

DEFINICIÓN. Una relación de orden en el conjunto A se denomina *relación de orden total en* A si esta se relaciona en A es decir, si para todos x, y de A se tiene.

$sea\ xRy, sea\ x = y, sea\ yRx.$

Una relación de orden no total es habitualmente llamada *relación de orden parcial u orden parcial.*

EJEMPLOS. 1. La relación "inferior a" del conjunto de números reales es una relación de orden total.

2. La relación de orden adoptada en los diccionarios en el idioma ruso, se denomina *lexicográfico*. El orden lexicográfico en el conjunto de las palabras del idioma ruso es un orden total.

3. La relación de inclusión $\subset$ en la colección de sub-conjunto de un conjunto dado M es una relación de orden parcial si M consta al menos de dos elementos diferentes.

Un mismo conjunto puede ser totalmente ordenado por las relaciones de orden diferentes. Es también, por ejemplo, que en el conjunto finito M no vacío compuesto de n elementos se aplica aplicar $n!$ Orden totales diferentes.

Conjunto ordenado. Sea R una relación de orden cualquiera en el conjunto A no vacío.

DEFINICIÓN. Se denomina *conjunto ordenado* el par $\langle A, R\rangle$, donde A es un conjunto no vacío y una relación de orden en A. Si el orden R sobre A es total, el par $\langle A, R\rangle$ se denomina *conjunto totalmente ordenado*. Si el orden R sobre A es parcial, entonces la pareja $\langle A, R\rangle$, se denomina *conjunto parcialmente ordenado.*

DEFINICIÓN. Sea $\langle A, \quad \rangle$ un conjunto ordenado. El elemento a de A se denomina *mínimo (máximo) elemento* de A si $a \quad x\ (x \quad a)$ para todo elemento x de A diferente de a.

Todo conjunto ordenado no contiene más de un pequeño elemento y de un mayor elemento.

DEFINICIÓN. Sea $\langle A, \quad \rangle$ un conjunto ordenado. El elemento a es llamado minimal (maximal) en A en caso donde se satisface la condición: para todo x de A si x a, x $= a$ (si a x, entonces a $= x$).

Cualquier conjunto ordenado puede contener varios elementos minimales y maximales.

EJEMPLO. Sea R la relación de divisibilidad en el conjunto $\mathrm{N} \setminus \{0, 1\}$ (N es el conjunto de los números naturales). En el conjunto ordenado$\langle \mathrm{N} \setminus \{0, 1\}, R\rangle$ todo numero primo es un elemento minimal.

En un conjunto totalmente ordenado las nociones del elemento el más pequeño(es el mayor) y minimal (maximal) coinciden.

DEFINICIÓN. Un conjunto ordenado $\langle A, R\rangle$se denomina conjunto bien ordenado si cada sub-conjunto no vacío del conjunto A posee el primer elemento.

EJEMPLOS.1. si $<$ es la relación banal "inferior a" en el conjunto N de los números naturales, entonces, $\langle N, <\rangle$ es un conjunto bien ordenado.

2. Sea $<$ la relación banal "inferior a" en el conjunto R de todos los números reales. En ese caso el conjunto totalmente ordenado $\langle R, <\rangle$ no es un conjunto bien ordenado.

Ejercicios.

1. Demostrar que la función idéntica i_A del conjunto A es una relación de orden del conjunto A,
2. Mostrar que la relación

$$R = \{\langle x, y\rangle | x, y\ y \in \mathrm{N}\ x\ divide\ y\ o\ x < y\rangle\}$$

Es un orden total en el conjunto N de los números naturales.

3. Sea $A = \{1,2,3,4,5,6,7\}$ Y

$$R = \{\langle x, y\rangle | x,y\ y \in \text{A y } (x-y) \vdots 2\}$$

Mostrar que R es una relación de equivalencia en A.

4. Sea las relaciones $< y \leq$ definidas en el conjunto N de los números naturales de manera banal. Demostrar que $<\circ<\neq<; \leq\circ<=<; \leq\circ\geq= \text{N} \times \text{N}$

5. Construir un orden total en el conjunto $\text{N} \times \text{N}$.

6. Demostrar que un conjunto finito que contiene n elementos puede ser totalmente ordenado por $n!$ procedimiento.

7. Demostrar que la relación de inclusión $\subset$ no constituye a un orden total en la colección $P(A)$ de todos los sub-conjunto A del conjunto A, si A contiene menos de dos elementos.

8. Demostrar que todo conjunto bien ordenado es un conjunto totalmente ordenado.

9. Demostrar que la relación binaria R en el conjunto A es una relación de orden no estricta si solamente si $R \circ R = R\ y\ R \circ R^{-1} = i_A$.

10. Demostrar que si R es una relación de orden (orden total) la relación inversa R^{-1} es igualmente una relación de orden (orden total).

11. Sea $\leq$ una relación de orden no estricta en el conjunto A. Demostrar que la relación $<$ no es reflexiva y es transitiva en A.

12. Sea $<$una relación binaria no reflexiva y transitiva en el conjunto A.
Demostrar que la relación $\leq$ es tal que $x \leq y \equiv (x < y) \vee (x = y)$ es una relación de orden no estricta en A.

13. Demostrar que para un conjunto totalmente ordenado las nociones del más grande (el más pequeño) y de maximal (minimal) elementos coinciden.

14. Demostrar que si R es un orden parcial (orden total, bien ordenado), en el conjunto A y $B \subset A, R \cap (B \times B)$ es un orden parcial (total,) en el conjunto B.

15. Sea R la relación de pre orden en el conjunto A. plantéese $a \sim b \equiv\equiv (\langle a, b\rangle \in R \wedge \langle b, a\rangle \in$. Demostrar que:
(a) si $a \sim c, b \sim d, \langle a, b\rangle \in R$, entonces $\langle c, d\rangle \in R$;
(b) $\sim$ Es la relación de equivalencia en A.
(c) R_1 Es la relación de orden en $A/\sim$, donde $R_{1=\{\langle a/\sim, b/\sim\rangle}|\langle a, b\rangle \in R\}$.

CAPITULO III
ÁLGEBRA Y SISTEMAS ALGEBRAICOS

§ 1. Operaciones binarias

Operaciones binarias y n-áreas. Sea A un conjunto no vacío.

DEFINICIÓN. Llámese operación binaria del conjunto A a la función del conjunto $A \times A$ en A.

La adición y la multiplicación banales de los números enteros son EJEMPLOS de operaciones binarias en el conjunto de los enteros. Sea $P(M)$ el conjunto de todos los sub-conjunto del conjunto M; la reunión $\cup$ y la intersección $\cap$ son los EJEMPLOS de operación binaria en el conjunto P (M).

Sea ƒ una operación binaria cualquiera en el conjunto A. si en la función ƒ el elemento c corresponde al par $\langle a,b\rangle$, es decir, $\langle\langle a,b\rangle, c\rangle \in$ ƒ, entonces, en lugar de

$\mathfrak{f}(\langle a, b\rangle) = c$ O $\mathfrak{f}(a,b) = c$

Se escribe igualmente

$a\mathfrak{f}b = c$ O $\langle a,b\rangle \to c$,

El elemento c se denomina composición de elementos a y b.

DEFINICIÓN. Sea A^n la enésima potencia del conjunto no vacío A y $n \geq 1$. La aplicación del conjunto A^nen A se denomina n-área operación en el conjunto A, mientras que n es llamada rango de la operación. La operación nularia en el conjunto A se llama separación (fijación) de un cierto elemento A, el número 0 se denomina rango de la operación nularia.

DEFINICIÓN. La función del conjunto A^n en A se denomina operación n-área parcial en A si el dominio de DEFINICIÓN de la función no coinciden con A^n.

Las operaciones de rango o, 1 y 2 son igualmente llamados en un lugar, singular (unario) y binario respectivamente. La operación singular es también llamada operador.

EJEMPLOS. 1. La función asociada en cada conjunto A de P (M) son complementario $\mathrm{M} \setminus A$ es una operación singular (unario) en el conjunto P (M).

1. en el dominio de los números enteros naturales la sustracción no siempre es posible. Por tanto la sustracción en el conjunto de los números naturales es una operación binaria parcial.
2. La operación de división de los números racionales es una operación binaria parcial en el conjunto de los números racionales.
3. La operación que asocia cada cotejo de n de los números naturales máximo común divisor de estos números es una operación n-áreas en el conjunto de los números naturales.

Para ensenar una operación n-área utilizamos habitualmente la misma forma de notación que para las aplicaciones (de las funciones) cualquiera. Si $\mathfrak{f}$ es una operación n-área en el conjunto A y

$$\langle\langle a, \dots, a_n\rangle, a_n + 1\rangle \in \mathfrak{f},$$

Escribimos $a_n + 1 = \mathfrak{f}\left(a_{1,\dots,}a_n\right)$ y decimos que $a_n + 1$ es el valor de la operación $\mathfrak{f}$ para una variación de argumentos $a_{1,\dots,}a_n$.

Tipos de operaciones binarias. Sea $\intercal$ y $\perp$ de las operaciones binarias cualesquiera en el conjunto A.

DEFINICIÓN. La operación binaria $\intercal$ se denomina conmutativa si para todos a, b de A es

$$a \intercal b = b \intercal a.$$

DEFINICIÓN. La operación binaria $\intercal$ se denomina asociativa so para todos los elementos cualesquiera a, b, c, de A es $a \intercal (b \intercal c) = (a \intercal b) \intercal c$.

DEFINICIÓN. La operación binaria $\intercal$ se denomina distributiva relativamente en la operación binaria $\perp$ si para todo las a, b, c cualesquiera de A se satisface las igualdades

$(a \intercal b) \intercal c = (a \intercal c) \perp (b \intercal c)\ y\ c \intercal (a \intercal b) = (c \intercal a) \perp (c \intercal b)$.

Si la operación $\intercal$ es asociativa, podemos entonces suprimir los paréntesis y escribir $a \intercal b \intercal c$ en lugar de $a \intercal (b \intercal c)$O $a \intercal b) \intercal\intercal c$

EJEMPLOS 1. La adición y la multiplicación de los números racionales son las operaciones binarias conmutativas y asociativas.

2. la operación de sustracción en el conjunto de los números racionales no es conmutativa ni asociativa.

3. las operaciones reunión e intersección del sub-conjunto del conjunto M son conmutativa y asociativa en el conjunto P (M).

4. La composición defunciones es una operación asociativa.

La composición defunciones no es conmutativa: en caso general la igualdad $f \circ g = g \circ f$ no es válido.

5. Las operaciones reunión e intersección en el conjunto P (M) del sub-conjunto de algún conjunto son mutuamente distributiva el uno con referente al otro.

6. una multiplicación de enteros es distributiva en relación a la adición. Ahora bien, la adición de los enteros no es distributiva en relación a la multiplicación, pues en el caso general la igualdad $a + +bc(a + b)(a + c)$ no es válida.

Elementos neutros. Sea T una operación binaria en el conjunto A.

DEFINICIÓN. El elemento e de A se denomina elemento neutro a la izquierda relativamente a la operación T si para todo a de A se satisface la igualdad $e \ T \ a = a$. El elemento e de A es llamado elemento neutro a la derecha relativamente a la operación T si para todo elemento a de A en a varían las igualdades $e \ T \ a = a = a \ T$ e.

DEFINICIÓN. El elemento e de A se denomina elemento neutro relativamente a la operación T si para todo elemento a de A verifican las igualdades $e \ T \ a = a = a \ T$ e.

TEOREMA 1.1 si existe relativamente en la operación binaria T un elemento neutro, es entonces único.

Demostración. Siendo e y e′ los elementos neutros en relación aT. Entonces, e′ = e′ T e = e, es decir, e′ = e. □

COROLARIO. 1.2 si existe un elemento neutro relativamente en la operaciónT, entonces todos los elementos neutros a la izquierda y a la derecha con respecto a T coinciden con el.

EJEMPLOS. 1. El número 0 es un elemento neutro con respecto a la adición de los enteros. El número 1 es un elemento neutro con respecto a la multiplicación de los enteros.

2. un conjunto vacío es un elemento neutro relativamente a la operación reunión de conjunto. Un conjunto universal es un elemento neutro a la operación de intersección de conjunto.

3. consideramos el conjuntoΦ de aplicaciones de un conjunto no vacío A sobre su sub-conjunto propio no vacío B y la operación composición de aplicaciones. El conjuntoΦ no contiene ningún elemento neutro a la derecha. Todo elemento $\varphi \in \Phi$ tal que $\varphi(x) = x$ para un x cualquiera de B es un elemento neutro a la izquierda relativamente en la operación .

Elementos regulares. Sea T una operación binaria en el conjunto A.

DEFINICIÓN. El elemento $\alpha \in A$ se denomina elemento regular a la derecha relativamente en la operación T si para todo elemento b, c del conjunto A se deduce de $\alpha \ T \ b = \alpha \ T \ c$ que $b = c$. el elemento $\alpha \in A$ se denomina elemento regular a la izquierda con respecto a T, si para todo elemento b, c del conjunto A de $b \ T \ \alpha = c \ T \ \alpha$ $b = c$.

DEFINICIÓN. El elemento $\alpha \in A$ se denomina elemento regular relativamente en la operación T si es regular a la izquierda y a la derecha con respecto aT.

Ahora, si el elemento α es regular en las igualdades de tipo $\alpha \ T \ b == \alpha \ T \ c$ y $b \ T \ \alpha = c \ T \ \alpha$ podemos simplificar por α.

EJEMPLOS.1. Todo entero es regular con respecto a una adición.

2. Todo número entero diferente de cero es regular con respecto a la multiplicación; el número cero no es regular con respecto a una multiplicación.

TEOREMA. 1.3. Si los elementos α y b son regulares relativamente en una operación asociativa T, entonces su composición $\alpha \ T \ b$ es igualmente un elemento regular con respecto a T.

Demostración. Sea α y b los elementos regulares con respecto a T. suponemos que c, d son elementos de A correspondiente a la adición.

(1) $(\alpha \ T \ b) \ T \ c = (\alpha \ T \ b) \ T \ d$.

Ya que la operación T es asociativa, $a \ T \ (b \ T \ c) = a \ T \ (b \ T \ d)$.

En virtud de la regularidad del elemento a, en a $b \top c) = b \top d$. De donde, en virtud de la regularidad del elemento b, deducimos la igualdad

(2) $c = d$.

En resumen, para todo elemento c, d del elemento A (2) se deduce de (1), y por consiguiente el elemento $a \top b$ es regular a la derecha. De manera análoga nos damos cuenta que este elemento es regular a la izquierda □

Elementos simétricos. Sea ⊤ una operación binaria en el conjunto A que contiene un elemento neutro e.

DEFINICIÓN. El elemento v de A se denomina simétrico a la izquierda del elemento $\alpha \in A$ relativamente a la operación ⊤ si $v \top \alpha = e$. el elemento $v\ de\ A$ se denomina simétrico a la derecha de a relativamente en la operación ⊤ $si\ \alpha \top v = e$.

DEFINICIÓN. El elemento $\alpha' \in A$ se denomina simétrico del elemento $\alpha \in\in A$ relativamente en la operación ⊤ $si\ \alpha \top \alpha' = e = \alpha' \top \alpha$. En este caso el elemento α se denomina inversible, mientras que $\alpha\ y\ \alpha'$ son mutuamente inversos.

EJEMPLOS.1. con relación a la adición de enteros la simétrica de un entero dado es el mismo entero, pero con el mismo signo menos.

2. con relación a la multiplicación de los números racionales la simétrica de un número no nulo $\alpha\ es\ 1/\alpha$; el número cero no es simétrico en relación a la multiplicación.

TEOREMA. 1.4. Si la operación ⊤ es asociativa y el elemento α es inversible, existe entonces un elemento único simétrico de α.

Demostración. Sea v, v los elementos simétricos del elemento α en relación a ⊤, es decir,

$\alpha \top v = e = v \top \alpha$, $\alpha \top v = e = v \top \alpha$.

Entonces en virtud de la asociativa de ⊤

$v = v \top e = v \top (\alpha \top v) = (v \top \alpha) \top v = e \top v = v$,

Es decir, que $v = v$. □

COROLARIO. 1.5. Si el elemento α posee un elemento simétrico α' relativamente en la operación asociativa ⊤, todas las simétricas a la izquierda y a la derecha del elemento α coinciden entonces con el elemento α'.

TEOREMA. 1.6. Si los elementos α, b son inversibles relativamente en la operación asociativa ⊤, el elemento $\alpha \top b$, es entonces igualmente inversible y el elemento $b' \top \alpha'$ es simétrica de $\alpha \top b$.

Demostración. Sea $\alpha' y\ b'$ los elementos simétricos de $\alpha\ y\ b$ respectivamente. En virtud de la asociativa de⊤.

$(\alpha \top b) \top (b' \top \alpha') = ((\alpha \top b)) \top b') \top \alpha' = (\alpha \top (b \top b')) \top \alpha' = (\alpha \top e) \top \alpha' = \alpha \top \alpha' = e$.

Nos damos cuenta igualmente que $(b' \top \alpha') \top (\alpha \top b) = e$.

Por consiguiente, el elemento $\alpha \top b$ es inversible y el elemento $b' \top \alpha'$ es simétrico de $\alpha \top b$. □

TEOREMA. 1.7. Un elemento inversible relativamente en un operación asociativa ⊤ es un elemento regular con relación a ⊤.

Demostración. Sea α un elemento inversible y $\alpha \top b = a \top c$ para los elementos b, c del conjunto A. En ese caso si α' es un elemento simétrico de α, en a $\alpha' \top (\alpha \top b) = \alpha' \top \top (a \top c$). En virtud de la asociatividad de la operación ⊤, en a ($\alpha' \top \top \alpha) \top b = (\alpha' \top \alpha) \top c$.

Por consiguiente, $e \top b = e \top c$ y $b = c$. Nos damos cuenta de manera análoga que para todo los elementos b, c del conjunto A de la igualdad $b \top \alpha = c \top \alpha$ se deduce $b = c$. El elemento α por tanto es regular con respecto a ⊤. □

Sub-conjuntos cerrados en las operaciones. Sea ⊤ una operación binaria en el conjunto $A\ Y\ B \subset A$.

DEFINICIÓN. El sub-conjunto B del conjunto A se denomina cerrado en la operación ⊤ si para todos α, b de B el elemento $\alpha \top b$ pertenece a B.

Observamos que un su-conjunto vacío es cerrado en todas las operaciones ⊤.

EJEMPLOS.1. El conjunto de todos los números pares es cerrado con respecto a la adición y a la multiplicación de enteros.
2. El conjunto de todos los números impares es cerrado con respecto a la multiplicación, pero no con respecto a la adición de enteros.
3. El conjunto de todos los elementos (de A) regulares relativamente en la operación asociativa ⊤ es cerrado con respecto a ⊤.

Proposición. 1.8. El conjunto de todos los elementos inversibles relativamente a una operación binaria asociativa ⊤ es cerrada con respecto a ⊤.

La demostración de esta proposición se deriva directamente del TEOREMA 1.6.

Sea B un conjunto no vacío, $B \subset A$ que es cerrado en la operación ⊤.

Entonces estamos en condición de definir en B una operación binaria $\top'$ de la manera siguiente: $\alpha \top' b = \alpha \top b$ para α, b de B cualesquiera.

La operación $\top'$ se denomina restricción de la operación, ⊤ en el conjunto B, mientras que ⊤ es la continuación de la operación $\top'$ en la operación en el conjunto A.

Escritura aditiva y multiplicativa. Las escrituras más utilizadas para una operación binaria son las escrituras aditiva y multiplicativa. Con la forma de escritura aditiva la operación binaria ⊤ se denomina adición y se escribe $\alpha + b$ en lugar de $\alpha \top b$ que se denomina elemento $\alpha + b$ suma de $\alpha\ y\ b$. El elemento simétrico del elemento α es simbolizado $(-\alpha)$ y se denomina elemento opuesto en α.

Un elemento neutro con respecto a la adición se denota 0 y se denomina elemento cero con respecto a la adicion. Con la notación aditiva las propiedades asociativa y conmutativa se nota en la siguiente forma

$\alpha + (b + c) = (\alpha + b) + c, \qquad \alpha + b = b + \alpha.$

Con la escritura multiplicativa la operación binaria se denomina multiplicación y se escribe $\alpha \cdot b$ en lugar de $\alpha \top b$ lo llámese elemento $\alpha \cdot b$ producto de $\alpha\ y\ b$. El elemento simétrico de α se escribe α^{-1} y se denomina elemento inverso de α. un elemento neutro con respecto en la multiplicación se escribe e o 1 y es denominada elemento unitario o elemento unidad con respecto a la multiplicación. Con la escritura multiplicativa las propiedades asociativa y conmutativa se denotan de este modo.

$\alpha \cdot (b \cdot c) =\cdot c, \qquad \alpha \cdot b = b \cdot \alpha.$

La propiedad distributiva de la multiplicación con respecto a la adición se escribe de esta manera

$(\alpha + b) \cdot c = \alpha \cdot c + b \cdot c, \qquad c(\alpha + b) = c \cdot \alpha + c \cdot b.$

Congruencia. Sea R una relación de equivalencia en el conjunto A y ⊤ una operación binaria en A.

DEFINICIÓN. Una relación de equivalencia R se denomina congruencia relativamente en la operación ⊤ si para todos los elementos α, b, c, d del conjunto A de $\alpha R d$ y bRd se deduce $(\alpha \top b)R(c \top d)$.

TEOREMA. 1.9. Sea ⊤ una operación binaria en el conjunto A y R una congruencia con respecto a ⊤. Entonces, la igualdad

(1) $(\alpha/R)\ \top^*\ (b/R) = (\alpha \top b)/R,$

Donde $\alpha, b \in A,$ definimos la operación binaria $\top^*$ en el conjunto cociente $A\ /\ R$.

Demostración. La relación binaria $\top^*$ consta de dos pares de la forma

(2) $\langle\langle \alpha/R\,, b/R\rangle\,, \quad (\alpha \top b)/R\rangle, \quad \text{O } \alpha, b \in A.$

Se debe demostrar que $\top^*$ es una función. Sea.

$$\langle\langle c/R\,, d/R\,, \qquad (c \top d)/R\rangle \in \top^*.$$

Se debe demostrar que de la igualdad

(3) $\langle \alpha/R\,, b/R\rangle = \langle c/R\,, d\ /\ R\rangle$

Se deduce $(\alpha \top b)/R = (c \top d)/R$. De (3) se derivan las igualdades $\alpha/R = c/R$, $b/R = d/R$ y las relaciones (4)$\alpha R c$, bRd.

Dado que R es una congruencia con respecto en $\top$, de (4) se deduce:

$(\alpha \top b)\ R\ (c \top d)$ Y $(\alpha \top b)/R = (c \top d)/R$.

Por consiguiente, la relación $\top^*$ es una operación binaria en el conjunto cociente A/R. □

DEFINICIÓN. Una operación binaria $\top^*$ definida en un conjunto cociente A/R por la igualdad (1) se denomina operación asociada en la operación $\top$ por la congruencia R.

Ejercicios

1. Sea $\boldsymbol{N}^*$ El conjunto de todos los enteros positivos y $\top$ la operación en $\boldsymbol{N}^*$ de elevación a una potencia, es decir, que $\alpha \top b = \alpha^b$ para todos $\alpha, b \in \boldsymbol{N}^*$. Demostrar que la operación $\top$ no es conmutativa ni asociativa.
2. Sea α, b números racionales fijos. Demostrar que la función $\langle x,y\rangle \longmapsto \alpha x + by$, donde x, y son números racionales cualesquiera, es una operación binaria asociativa en el conjunto de números racionales.
3. Sea **N** el conjunto de todos los números naturales y (x, y) el máximo común divisor de los números naturales x y y. Demostrar que la función $\langle x,y\rangle \longmapsto (x, y)$ es una operación binaria conmutativa y asociativa en el conjunto **N.**
4. Sea $[x, y]$ el mínimo común múltiplo de los números naturales x y y.
   Demostrar que la función $\langle x,y\rangle \longmapsto [x, y]$ es una operación conmutativa y asociativa en el conjunto **N.**
5. Sea $P(U)$ un conjunto de todos los sub-conjunto del conjunto no vacío U. El conjunto $X \triangle Y$ definido por la formula
   $$X \triangle Y = (X \setminus Y) U (Y \setminus X)$$
   Se denomina diferencia simétrica de los conjuntos X y Y. Demostrar que $\triangle$ es una operación binaria conmutativa y asociativa en el conjunto $P(U)$. Demostrar que la operación $\cap$ es distributiva relativamente en la operación $\triangle$.
6. Dar un EJEMPLO del conjunto A, de relación de equivalencia R en A y de operación binaria $\top$ en A tal que
   (a) R sea una congruencia con respecto a $\top$.
   (b) R no es una congruencia con respecto a $\top$.

§2. Álgebra

Concepto de álgebra. Damos la definición de un concepto fundamental en álgebra.

DEFINICIÓN. Se denomina álgebra un par ordenado $\mathcal{A} = \langle A, \Omega\rangle$, donde A es un conjunto no vacío y Ω el conjunto de operaciones en A.

Por lo tanto el álgebra $\mathcal{A}$ se define por dos conjuntos:

(a) Un conjunto no vacío A se denota igualmente $|\mathcal{A}|$; este conjunto se denomina conjunto fundamental(conjunto de base) de álgebra $\mathcal{A}$ y sus elementos se denominan elementos de álgebra $\mathcal{A}$;

(b) Un conjunto de operaciones Ω definidos en A y llamados operaciones principales de álgebra $\mathcal{A}$.

Si $\langle A, \Omega\rangle$ es una álgebra, se dice que el conjunto A es una álgebra relativamente en las operaciones Ω.

DEFINICIÓN. Las álgebras $\mathcal{A} = \langle A, \Omega\rangle, = B, \Omega'$ se denominan <u>del mismo tipo</u>, si existe una función inyectiva del conjunto Ω en Ω' por lo cual toda operación $\mathfrak{f}_{\mathcal{A}}$ de Ω, que corresponda en la función, que posea el mismo rango. El caso más general es del conjunto donde el conjunto Ω es finito, es decir, $\Omega = \{\mathfrak{f}_1, \dots, \mathfrak{f}s\}$. En ese caso en lugar de la notación $\mathcal{A} = \langle A, \{\mathfrak{f}_1, \dots, \mathfrak{f}s\}\rangle$

Escribimos habitualmente

$\mathcal{A} = \langle A, \mathfrak{f}_1, \dots, \mathfrak{f}s\rangle$.

Si entre las operaciones principales $f_{1,\dots,}f_s$ del álgebra hay operaciones en ningún lugar, por EJEMPLO, $f_{r+1}, \dots, f_s$, y $a_{r+1}, \dots, a_s$ que son elementos separados de $|\mathcal{A}|$, utilizamos también la notación

$$\mathcal{A} = \langle A, f_1, \dots, f_r, a_{r+1}, \dots, a_s \rangle.$$

En ese caso los elementos separados $a_{r+1}, \dots, a_s$ que constituyen los valores de operaciones principales en ningún lugar, se denominan elementos separados o elementos principales del álgebra $\mathcal{A}$.
Se denomina tipo de álgebra $\mathcal{A} = \langle A, f_1, \dots, fs \rangle$ la serie $(r(f_1), \dots, r(f_s))$ donde $r(f_i)$ es el rango de la operación f_i. Las álgebras $\mathcal{A}$ y $\mathfrak{B} = \langle B, f'_1, \dots, f'_s \rangle$ son del mismo tipo en caso que coincida, es decir, en caso donde el rango de la operación f_i coincide con el rango de la operación f'_1 por $i = 1, \dots, s$
EJEMPLOS.1. sea $+$ y $\cdot$ (adición y multiplicación) las operaciones aritméticas en el conjunto $\mathbf{Z}$ de enteros. El álgebra $\langle \mathbf{Z}, +, \cdot \rangle$ es un álgebra de tipo (2,2)
2. sea $+ \; y \; \cdot$ de las operaciones aritméticas en el conjunto $\boldsymbol{N}$ de números naturales. El álgebra $\langle \boldsymbol{N}, +, \cdot \rangle$
Es un álgebra de tipo (2,2).

3. Sea P (U) un conjunto de todos los sub-conjunto de un conjunto no vacío U y $\cap, U, '$ de operaciones intersección, reunión y complementación en el sub-conjunto del conjunto U. El álgebra $\langle P(U), \cap, U, ' \rangle$ es un álgebra de tipo (2, 2,1).
DEFINICIÓN. Un álgebra $\mathcal{A} = \langle A, *, e \rangle$ del tipo (2.0), donde Aes un conjunto cualquiera no vacío, $*$ una operación binaria asociativa en A, e un elemento neutro con respecto a $*$, se denomina monoide.
EJEMPLO. Sea M un conjunto finito cualquiera no vacío, A el conjunto de todas las funciones M en M, $*$ una operación de composición defunciones de M en M, i_M una función idéntica de M en M, entonces, $\langle A, *, i_A \rangle$ es un monoide.

Homomorfismo de álgebra. Sea $\mathcal{A} \; y \; \mathfrak{B}$ álgebras de un mismo tipo, f_A una operación principal cualquiera de álgebra $\mathcal{A}$ y $f_{\mathfrak{B}}$ la operación principal que le corresponde $\mathfrak{B}$.
Se dice que la función h del conjunto $|\mathcal{A}|$ en el conjunto $|\mathfrak{B}|$ con respecto a la operación f_A del álgebra $\mathcal{A}$ si

(1) $h(f_{\mathcal{A}}(\alpha_1, \dots, \alpha_{m)}) = f_{\mathfrak{B}}(h(\alpha_1), \dots, h(\alpha_m))$
Para todos $\alpha_1, \dots, \alpha_m$ de $|\mathcal{A}|$,
Donde m es el rango de la operación $f_{\mathcal{A}}$.
Distíngase el caso donde $f_{\mathcal{A}}$ es una operación nularia, es decir, que ella separa un elemento cualquiera α del álgebra $\mathcal{A}$. La operación$f_{\mathfrak{B}}$ que le corresponde será entonces igualmente una operación nularia, que por consiguiente separa un elemento cualquiera b del álgebra $\mathfrak{B}$. En ese caso la condición (1) adoptara la forma

$h(\alpha) = b,$

Es decir, que el elemento separado α del álgebra $\mathcal{A}$ proviene de la función h el elemento b del álgebra $\mathfrak{B}$.

DEFINICIÓN. Se denomina <u>homomorfismo del álgebra</u> $\mathcal{A}$ en (sobre) el álgebra del mismo tipo $\mathfrak{B}$ talfunción h del conjunto $|\mathcal{A}|$ en (sobre) $|\mathfrak{B}|$ que respeta todas las operaciones principales del álgebra , $\mathcal{A}$, es decir, que satisface a la condición (1) para toda operación principal $f_{\mathcal{A}}$ del álgebra $\mathcal{A}$. El homomorfismo del álgebra $\mathcal{A}$ en $\mathfrak{B}$ se denomina epimorfismo.

DEFINICIÓN. El homomorfismo h del álgebra $\mathcal{A}$ en el álgebra $\mathfrak{B}$ se denomina isomorfismo si h es una función inyectiva del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$. Las álgebras $\mathcal{A}$ y $\mathfrak{B}$ se denominan isomorfismo si hay isomorfismo de $\mathcal{A}$ en $\mathfrak{B}$.
La notación $\mathcal{A} \cong \mathfrak{B}$ significa que las álgebras $\mathcal{A}$ y $\mathfrak{B}$ son isomorfismos.

DEFINICIÓN. El homomorfismo h del álgebra $\mathcal{A}$ en álgebra $\mathfrak{B}$ se denomina monomorfismo o inyección si h es una función inyectiva del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$.

DEFINICIÓN. El homomorfismo del álgebra $\mathcal{A}$ en si misma se denomina endomorfismo de álgebra $\mathcal{A}$. El isomorfismo del álgebra $\mathcal{A}$ en si misma se denomina automorfismo del álgebra $\mathcal{A}$.

Así por ejemplo, el automorfismo del álgebra $\mathcal{A}$ es una función idéntica del conjunto $|\mathcal{A}|$ sobre el mismo.

EJEMPLO. Sea $\dashv\cdot$ la operación de adición en el conjunto **R** de números reales y $\cdot$ la operación de multiplicación en el conjunto $\boldsymbol{R}^*$ de los números reales positivos. Cada una de las álgebras $\langle \boldsymbol{R}^*, ., 1\rangle$ y $\langle \boldsymbol{R}, +, 0\rangle$ es un tipo (2,0). Muéstrese que son isomorfas.

Considérese la función h:

$h(x) = \log x$ Para todo x de $\boldsymbol{R}^*$.

Vemos fácilmente que h es lafunción de $\boldsymbol{R}^*$ en **R**. la función h es inyectiva, ya que para todo x, y de $\boldsymbol{R}^*$ se satisface la condición: si $\log x = \log y$ entonces $x = y$. Además, $h = (1) = 0$ y para todo x, y y de $\boldsymbol{R}^*$ se tiene $\log(xy) = \log x + \log y$, es decir, que $h(x, y) = h(x) + h(y)$. Por consiguiente la función h respeta las principales operaciones del álgebra $\langle \boldsymbol{R}^*, ., 1\rangle$. Por tanto, h es un isomorfismo de la primera álgebra sobre la segunda.

TEOREMA. 2.1 sea h un homomorfismo del álgebra $\mathcal{A}$ en álgebra $\mathfrak{B}$y g un homomorfismo del álgebra $\mathfrak{B}$ en álgebra c. (Esa c no es no la encontré)

Su composición g ∘ h es entonces un homomorfismo del álgebra $\mathcal{A}$ en álgebra c.

Demostración. Sea $\mathfrak{f}_{\mathcal{A}}$una operación principal cualquiera del álgebra $\mathcal{A}$(de rango $m > 0$), $\mathfrak{f}_{\mathfrak{B}}$ la operación principal asociada del álgebra $\mathfrak{B}$ y $\mathfrak{f}_c$ la operación principal del álgebra c que corresponde a la operación $\mathfrak{f}_{\mathfrak{B}}$. Se debe demostrar que para todos los elementos $\alpha_1, \dots, \alpha_m$ de $|\mathcal{A}|$, se tiene

(1) $\quad \mathrm{g} \circ h\big(\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m)\big) = \mathfrak{f}_c(\mathrm{g} \circ h(\alpha_1), \dots, \mathrm{g} \circ h(\alpha_m))$.

Por definición de la composición defunciones

$\mathrm{g} \circ h(\alpha_1, \dots, \alpha_m)) = \mathrm{g}\ \left(h\left(\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m)\right)\right)$.

Ahora bien, como por hipótesis h y g son homomorfismos, se tiene

$$\mathrm{g}(h(\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m))\big) = \mathrm{g}\ (\mathfrak{f}_{\mathfrak{B}}(h(\alpha_1), \dots, h\left(\alpha_m\right))\big) =$$
$$= \mathfrak{f}_c(\mathrm{g}\big(h(\alpha_1)\big), \dots, \mathrm{g}\left(h\left(\alpha_m\right)\right)\big) =$$
$$= \mathfrak{f}_c\left((\mathrm{g} \circ h)(\alpha_1), \dots, (\mathrm{g} \circ h)(\alpha_m)\right).$$

Por consiguiente la igualdad (1) es válida. Para las operaciones principales nularias, los razonamientos son idénticos. □

TEOREMA2.2. Sea h un homomorfismo del álgebra $\mathcal{A}$ en álgebra $\mathfrak{B}$ y g un homomorfismo del álgebra $\mathfrak{B}$ en álgebra c.

Su composición g ∘ h es entonces un homomorfismo del álgebra $\mathcal{A}$ en álgebra c.

Este TEOREMA se deriva directamente del TEOREMA 2.1 del TEOREMA 2.3.4.

TEOREMA2.3 Sea h un isomorfismo del álgebra $\mathcal{A}$ en álgebra $\mathfrak{B}$ y g un isomorfismo del álgebra $\mathfrak{B}$ en álgebra c. su composición g ∘ h es entonces un isomorfismo del álgebra $\mathcal{A}$ en álgebra c.

Demostración. Según el TEOREMA 2.1 se deriva de la hipótesis que g ∘ h es un homomorfismo del álgebra $\mathcal{A}$ en álgebra c. luego, por la hipótesis h es una función inyectiva del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$ y g una función inyectiva del conjunto $|\mathfrak{B}|$en $|c|$. Según los TEOREMAs 2.3.9 y 2.3.4 se deduce que g ∘ h es una función inyectiva del conjunto $|\mathcal{A}|$ en $|c|$.

Así que g ∘ h es un isomorfismo del álgebra $\mathcal{A}$ en álgebra c. □

TEOREMA 2.4. Sea h un isomorfismo del $\mathcal{A}$ en álgebra $\mathfrak{V}$. La función h^{-1} es entonces un isomorfismo del álgebra $\mathfrak{B}$ en álgebra $\mathcal{A}$.

Demostración. Por hipótesis h es una función inyectiva del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$ por consiguiente el corolario 2.3.14, h^{-1} es una función inyectiva de $|\mathfrak{B}|$ en $|\mathcal{A}|$.

Sea $\mathfrak{f}_{\mathcal{A}}$ una operación principal cualquiera del álgebra $\mathcal{A}$ (de rango m) y $\mathfrak{f}_{\mathfrak{B}}$ una operación principal apropiada del álgebra $\mathfrak{V}$. Solo se tiene que demostrar que para todos los elementos $b_1, \dots, b_m$ de $|\mathfrak{B}|$, se tiene

(1) $h^{-1}\mathfrak{f}_{\mathfrak{B}}(b_1, \dots, b_m)\big) = \mathfrak{f}_{\mathcal{A}}\big(h^{-1}(b_1), \dots, h^{-1}\big(b_m\big)\big)$.

Esta condición es equivalente a la siguiente:

(2) $h(\mathfrak{f}_{\mathcal{A}}(h^{-1}(b_1), \dots, h^{-1}\left(b_m\right))\big) = \mathfrak{f}_{\mathfrak{B}}(b_1, \dots, b_m)$.

Ahora bien, como por hipótesis h es un homomorfismo del $\mathcal{A}$ en álgebra $\mathfrak{V}$, se tiene

$$h(\mathfrak{f}_{\mathcal{A}}(h^{-1}(b_1), \dots, h^{-1}\left(b_m\right))\big) = \mathfrak{f}_{\mathfrak{B}}\big(h\big(h^{-1}\big(b_1\big)\big), \dots,$$
$$\dots, h\left(h^{-1}\left(b_m\right)\right)\big) = \mathfrak{f}_{\mathfrak{B}}(b_1, \dots, b_m).$$

Es decir, que (2) es válida y por consiguiente, (1) también.

Por lo tanto h^{-1} es un isomorfismo del álgebra $\mathfrak{V}$ en álgebra $\mathcal{A}$. □

TEOREMA 2.5. Una relación de isomorfismo en el conjunto cualquiera de álgebras es una relación de equivalencia.

Demostración. Una función idéntica $\mathcal{A}$ en álgebra $\mathcal{A}$, es decir, una función h tal que $h = (\alpha) = \alpha$ cualquiera que sea α de $|\mathcal{A}|$, es aparentemente un isomorfismo del álgebra $\mathcal{A}$ en $\mathcal{A}$. Según el TEOREMA 2.3 la relación de isomorfismo es transitiva. Según el TEOREMA 2.4 la relación de isomorfismo es simétrica, ya que la relación de isomorfismo es una relación de equivalencia. □

Sub-álgebras. Sea f una operación n-áreas en el conjunto A y B un sub-conjunto no vacío del conjunto A. de acuerdo con el concepto de restricción de una función en un conjunto decimos que una operación n-área g en B es una restricción de la operación f en el conjunto B si

$\mathrm{g}\big(b_{1,\dots,}b_n\big) = \mathrm{f}(b_1, \dots b_n)$ para todos $b_{1,\dots,}b_n$de B.

En particular, una operación nularia g en B es una restricción f en A en el conjunto B es una restricción de la operación nularia f en $\mathcal{A}$ en el conjunto $\mathfrak{B}$, si

g= f, es decir, si g y f separan un mismo elemento respectivamente en B y A. La restricción de la operación f por el conjunto B será designada por el símbolo f $|B$.

Sea $\mathcal{A} = \langle A, \Omega\rangle$ y $\mathfrak{B} = \langle B, \Omega^{'}\rangle$de álgebras del mismo tipo.

DEFINICIÓN. El álgebra $\mathfrak{B}$ se denomina sub-álgebra de un álgebra del mismo tipo $\mathcal{A}$ si $B \subset A$ y la función idéntica del conjunto B en A es un monomorfismo del álgebra $\mathfrak{B}$ en álgebra $\mathcal{A}$, es decir, para cada operación principal $\mathfrak{f}_{\mathfrak{B}}$ del álgebra $\mathfrak{V}$ se tiene

$\mathfrak{f}_{\mathfrak{B}(b_1,\dots,b_m)}=\mathfrak{f}_{\mathcal{A}}(b_1,\dots,b_m)$

Para todos $b_1, \dots, b_m$ de B,

Donde m es el rango de la operación $\mathfrak{f}_{\mathcal{A}}$ mientras que $\mathfrak{f}_{\mathfrak{B}}$ es la operación principal del álgebra $\mathfrak{V}$ que corresponde en $\mathfrak{f}_{\mathcal{A}}$.

Recordemos que para la función idéntica del conjunto B en A entendemos una función h tal que $h(\quad) = b$ cualquiera que sea el elemento b de B.

Se muestra sin problema que la definición de sub-álgebra dada anteriormente es equivalente al enunciado siguiente: el álgebra $\mathfrak{B}$ se denomina sub-álgebra del álgebra del mismo tipo $\mathcal{A}$ si $B \subset A$ y cada operación principal $\mathfrak{f}_{\mathfrak{B}}$ del álgebra $\mathfrak{B}$ es una restricción de la operación correspondiente $\mathfrak{f}_{\mathcal{A}}$ del álgebra $\mathcal{A}$ del conjunto B.

La notación $\mathfrak{B}$ $\mathcal{A}$ significa que el álgebra $\mathfrak{B}$ es un sub-álgebra de álgebra $\mathcal{A}$.
Sea $\mathcal{A} = \langle A, \Omega \rangle$ un álgebra $B \subset A$.

DEFINICIÓN. Un sub-conjunto B del conjunto $|\mathcal{A}|$ se denomina cerrado en álgebra $\mathcal{A}$ si B es cerrado relativamente en cada operación principal $\mathfrak{f}_{\mathcal{A}}$ del álgebra $\mathcal{A}$, es decir, si se tiene
(1) $\mathfrak{f}_{\mathcal{A}}(b_1, \dots, b_m) \in B$ Para todos $b_1, \dots, b_m$ de B,
Donde m es el rango de la operación nularia, la condición (1) adopta la forma $\mathfrak{f}_{\mathcal{A}} \in B$.
Por supuesto sea que si $\mathfrak{B}$ $\mathcal{A}$ entonces el conjunto $|\mathfrak{B}|$ es cerrado en álgebra $\mathcal{A}$.
A partir de las DEFINICIÓNes dadas anteriormente se deriva directamente el TEOREMA siguiente.

TEOREMA. 2.6. Sea $\mathcal{A} = \langle A, \mathfrak{f}_1, \dots, \mathfrak{f}_S \rangle$ un álgebra y B un sub-conjunto no vacío del conjunto A cerrado en álgebra $\mathcal{A}$. En ese caso el álgebra

(2) $\mathfrak{V} = \langle B, \mathfrak{f}_1 | B, \dots, \mathfrak{f}_s | B \rangle$ es un sub-álgebra del álgebra $\mathcal{A}$.

Ya que el sub-conjunto no vacío B del conjunto $|\mathcal{A}|$ cerrado en álgebra $\mathcal{A}$ definido de manera univoca (anterior mente mencionada) el sub-álgebra $\mathfrak{V}$, se utiliza por esta sub-álgebra en lugar de la notación (2) la notación

$\mathfrak{V} = \langle B, \mathfrak{f}_1, \dots, \mathfrak{f}_s \rangle$.

Ejemplos.1. sea + y. (adición y multiplicación) las operaciones aritméticas usuales en el conjunto **Z** de enteros y **N** un conjunto de números naturales. En ese caso el álgebra $\langle \mathbf{N}, +, . \rangle$ Es entonces un sub-álgebra de álgebra $\langle \mathbf{Z}, +, . \rangle$.
2. Sea P (U) el conjunto de todos los sub-conjuntos del conjunto no vacío U, mientras que ∩,∪ y ´ son respectivamente las operaciones de intersección, reunión y complementación. El álgebra $\langle \{\emptyset, U\}, \cap, \cup, ´ \rangle$ es un sub-álgebra de álgebra $\langle P(U), \cap, \cup, ´ \rangle$.

TEOREMA. 2.7. Si $\mathcal{A}$ es un sub-álgebra del álgebra $\mathfrak{V}$ y $\mathfrak{V}$ un sub-álgebra del álgebra c, $\mathcal{A}$ es entonces un sub-álgebra del álgebra c.
Demostración. Sea $\mathcal{A}$ $\mathfrak{B}$. En ese caso $|\mathcal{A}| \subset |\mathfrak{B}|$ y
(1) $\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m) = \mathfrak{f}_{\mathfrak{B}}(\alpha_1, \dots, \alpha_m) \in \mathcal{B}$para todo $b_1, \dots, b_m$ de B,
donde $\mathfrak{f}_{\mathcal{A}}$ es una operación principal cualquiera del álgebra $\mathcal{A}$ y m su rango, mientras que $\mathfrak{f}_{\mathfrak{B}}$ es la operación apropiada del álgebra $\mathfrak{V}$. Así que, si $\mathfrak{V}$ c, se tiene $|\mathfrak{B}| \subset |c|$ y
(2) $\mathfrak{f}_{\mathfrak{B}}(\alpha_1, \dots, \alpha_m) = \mathfrak{f}_c(\alpha_1, \dots, \alpha_m)$
Para todo $\alpha_1, \dots, \alpha_m$ de $|\mathfrak{B}|$,
Donde $\mathfrak{f}_c$es la operación principal del álgebra c correspondiente a la operación $\mathfrak{f}_{\mathfrak{B}}$. Por consiguiente $|\mathcal{A}| \subset |c|$ y en virtud de (1), (2)

$$\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m) = \mathfrak{f}_c(\alpha_1, \dots, \alpha_m)$$

Para todos $\alpha_1, \dots, \alpha_m$ de $|\mathcal{A}|$.
Por consiguiente, $\mathcal{A}$ es un sub-álgebra del álgebra c. □

TEOREMA 2.8. La relación binaria (ser un sub-álgebra)
En el conjunto de sub-álgebras del álgebra $\mathcal{A}$ es una relación de orden no estricta.
Demostración. Una función idéntica del conjunto $|\mathcal{A}|$ en $|\mathcal{A}|$ es un monomorfismo del álgebra $\mathcal{A}$ en $\mathcal{A}$. Por consiguiente, $\mathcal{A}$ $\mathcal{A}$, la relación …. Por tanto es reflexiva. En virtud del TEOREMA 2.7 la relación …. Es transitiva.
Muéstrese que la relación …. Es anti simétrica. Admítase que los sub-álgebras $\mathfrak{B}$ y c del álgebra $\mathcal{A}$ satisfacen a las condiciones
(1) $\mathfrak{B}$ c y c $\mathfrak{B}$.
Entonces $|\mathfrak{B}| \subset |c|, |c| \subset |\mathfrak{B}|$ y, como resultado
(2) $|\mathfrak{B}| = |c|$.
Luego, en virtud de (1) para una operación principal cualquiera $\mathfrak{f}_{\mathfrak{B}}$ del álgebra $\mathfrak{B}$ se tiene

(3) $\mathfrak{f}_{\mathfrak{B}}(b_1, \dots, b_m) = \mathfrak{f}_c(b_1, \dots, b_m)$

Para todos $b_1, \dots, b_m$ de $|\mathfrak{B}|$,

Donde m es el rango de la operación $\mathfrak{f}_{\mathfrak{B}}$. En virtud de (2) y (3) se tiene

(4) $\mathfrak{f}_{\mathfrak{B}} = \mathfrak{f}_c$ para toda operación principal $\mathfrak{f}_{\mathfrak{B}}$ del álgebra $\mathfrak{B}$.

Tomamos sobre la base de (2) y (4) se concluye que $\mathfrak{B} = c$. Ya que, la relación …. es anti simétrica.

En resumen se ha demostrado que la relación …. Es reflexiva, transitiva y anti simétrica, es por lo tanto una relación de orden no estricto. □

TEOREMA 2.9. La intersección de una colección cualquiera de sub-conjunto $|\mathcal{A}|$ cerrado en álgebra $\mathcal{A}$ es un conjunto cerrado en álgebra $\mathcal{A}$

Demostración. Sea $\{C_i | i \in \boldsymbol{I}\}$ una colección cualquiera de sub-conjuntos C_i del conjunto $|\mathcal{A}|$ cerrado en álgebra $\mathcal{A}$ Yy $C = \cap C_i$. si C $= \emptyset$ el TEOREMA es válido ya que un conjunto vacío es $\boldsymbol{i} \in \boldsymbol{I}$

Cerrado en $\mathcal{A}$. Véase el caso donde $C \neq \emptyset$. Sea $\mathfrak{f}_{\mathcal{A}}$ una operación principal cualquiera de álgebra $\mathcal{A}$, m su rango y $c_1, \dots, c_m$

De elementos cualesquiera del conjunto C. En ese caso

(1) $\mathfrak{f}_{\mathcal{A}}(c_1, \dots, c_m) \in C_i$ para cada $i\ de\ \boldsymbol{I}$,

Dado que el conjunto c_1 es cerrado relativamente en la operación $\mathfrak{f}_{\mathcal{A}}$. En virtud de (1)

$$\mathfrak{f}_{\mathcal{A}}(c_1, \dots, c_m) \in \cap\, C_i = C,$$
$$\boldsymbol{i} \in \boldsymbol{I}$$

Es decir, que el conjunto C es cerrado relativamente en todas las operaciones principales de álgebra $\mathcal{A}$.■

Sea $\mathcal{A}$ un álgebra

(I) $\{\mathcal{A}_i | i \in \boldsymbol{I}\}$

Una colección cualquiera de los sub-álgebras $\mathcal{A}_i$ de álgebra $\mathcal{A}$ tal que $\cap\, |\mathcal{A}_i|$ sea un $\boldsymbol{i} \in \boldsymbol{I}$

Conjunto no vacío.

DEFINICIÓN. Se denomina intersección de la colección (I) de sub-álgebras de álgebra $\mathcal{A}$ el sub-álgebra $\mathfrak{B}$ de álgebra $\mathcal{A}$ tal que

$|\mathfrak{B}| = \cap\, |\mathcal{A}_i|$.

$i \in I$

La buena justificación de esta definición se deriva por el hecho que (en virtud del TEOREMA 2.9) el conjunto

$|\mathfrak{B}| = \cap\, |\mathcal{A}_i|$

$\boldsymbol{i} \in \boldsymbol{I}$

Es cerrado en álgebra $\mathcal{A}$ y el sub-conjunto $|\mathfrak{B}|$ no vacío y cerrado en álgebra $\mathcal{A}$ del conjunto $|\mathcal{A}|$(en virtud del TEOREMA 2.6) define de manera única el sub-álgebra $\mathcal{A}$ en un conjunto de base $|\mathfrak{B}|$.

La notación $\mathfrak{B} = \cap\, \mathcal{A}_i$ significa que el álgebra $\mathfrak{B}$ es una intersección de la colección (I) de los sub-álgebras $\mathcal{A}_i$ de álgebra $\mathcal{A}$.

En resumen, si (I) es una colección cualquiera de sub-álgebras de álgebra $\mathcal{A} = \langle A, f_1, \dots, f_s \rangle$ tal que $\cap\, |\mathcal{A}_i| \neq \emptyset$, el álgebra $\mathfrak{B}$

$\mathfrak{B} = \langle B, f_1 | B, \dots, f_s | B \rangle$,

Donde $B = \cap\, |\mathcal{A}_i|$, es entonces la intersección de álgebras de la colección (I).

$i \in I$

TEOREMA. 2.10. Si en álgebra $\mathcal{A}$entre las operaciones principales encontramos al menos una nularia, la intersección de una colección cualquiera (no vacío) de sub-álgebras de álgebra $\mathcal{A}$ es entonces un sub-álgebra de álgebra $\mathcal{A}$.

Demostración. En efecto, si $\{\mathcal{A}_i | i \in \boldsymbol{I}\}$ es una colección cualquiera de sub-álgebras de álgebra $\mathcal{A}$ que contiene al menos una operación principal nularia $\mathfrak{f}_{\mathcal{A}}$, el conjunto $B = \cap |\mathcal{A}_i|$ es $i \in I$

Entonces no vacío, puesto que contiene un elemento separado por la operación $\mathfrak{f}_{\mathcal{A}}$. En ese caso el conjunto B cerrado en $\mathcal{A}$ define (en virtud del TEOREMA 2.6) de manera única el sub-álgebra del álgebra $\mathcal{A}$ en el conjunto de base B. ■

Se deduce de la definición de sub-álgebra que para todo conjunto no vacío M de elementos de álgebra $\mathcal{A}$ dado, $M \subset |\mathcal{A}|$, existe un sub-álgebra minimal $\mathfrak{B}$ que incluye M. se observa fácilmente que una tal sub-álgebra es intersección de todas las sub-álgebras $\mathcal{A}$ que comporta el conjunto M. Esta sub-álgebra minimal $\mathfrak{B}$ se denomina sub-álgebra generado por el conjunto M, M siendo un sistema de generatrices de álgebra $\mathfrak{B}$.

Álgebra cociente. Sea $\mathcal{A}$ un álgebra y *R* una relación de equivalencia en el conjunto $|\mathcal{A}|$.

DEFINICIÓN. La relación *R* se denomina congruencia o congruencia en álgebra $\mathcal{A}$ si *R* es una congruencia relativamente en cada operación principal $\mathfrak{f}_{\mathcal{A}}$ de álgebra $\mathcal{A}$, es decir, que para todos los elementos $\alpha_1, \dots, \alpha_m, b_m$ del conjunto $|\mathcal{A}|$

(1) $\alpha_1 R B_1, \dots, \alpha_m R\, b_m$

Implica

(2) $f_{\mathcal{A}}(\alpha_1, \dots, \alpha_m)\, R f_{\mathcal{A}}(b_1, \dots, b_m)$,

Donde m es el rango de la operación $f_{\mathcal{A}}$.

Sea $\mathcal{A} = \langle A, \Omega \rangle$ un álgebra, *R* una congruencia en $\mathcal{A}$ y A / R un conjunto cociente del conjunto $A\ en\ R$ definamos en el conjunto A / R una operación m- área $f_{\mathcal{A}/R}$ que corresponde a la operación $f_{\mathcal{A}}$ de Ω de la forma siguiente:

(3) $f_{\mathcal{A}/R}(\alpha_1/R, \dots, \alpha_m / R) = f_{\mathcal{A}(\alpha_1,\dots,\alpha_m)} / R$

Para todos $\alpha_1, \dots, \alpha_m$ de A.

La definición es correcta, puesto que, en virtud de (2), el valor del segundo miembro de (3) es independiente de la elección de elementos $\alpha_1, \dots, \alpha_m$ respectivamente en las clases de equivalencia $\alpha_1/R, \dots, \alpha_m / R$(ver demostración del TEOREMA 1.9) la operación $f_{\mathcal{A}/R}$ se denomina operación asociada en la operación $f_{\mathcal{A}}$ por la congruencia R. nótese Ω^* el conjunto de todas las operaciones asociadas en las operaciones principales de álgebra $\mathcal{A}$ por la congruencia $R, \Omega^* = \{f_{\mathcal{A}/R} | f_{\mathcal{A}} \in \Omega\}$.

DEFINICIÓN. Sea $\mathcal{A} = \langle A, \Omega \rangle$ un álgebra y *R* una congruencia en $\mathcal{A}$. El álgebra $\langle \mathcal{A} / R, \Omega^* \rangle$ se denomina álgebra cociente de álgebra $\mathcal{A}$ en congruencia *R* se denota A / R.

TEOREMA 2.11. Sea *R* una congruencia en álgebra A. La función h del conjunto $|\mathcal{A}|$ en $|\mathcal{A}| / R$ es entonces tal que

(1) $h(\alpha) = \alpha / R$ para todo α de $|\mathcal{A}|$

Es un homomorfismo de álgebra $\mathcal{A}$ en álgebra cociente A / R.

Demostración. Se deduce de (1) que h es una función de $|\mathcal{A}|$ en $|\mathcal{A}| / R$. Es necesario demostrar que h respeta todas las operaciones principales de álgebra $\mathcal{A}$. Sea $f_{\mathcal{A}}$ una operación principal cualquiera de álgebra $\mathcal{A}$ y $f_{\mathcal{A}/R}$ la operación principal asociada de álgebra cociente A / R. Entonces, en virtud de (1), para todos $\alpha_1, \dots, \alpha_m$ de $|\mathcal{A}|$ se tiene

$$h(\mathfrak{f}_{\mathcal{A}}(\alpha_1, \dots, \alpha_m)) = f_{\mathcal{A}}(\alpha_1, \dots, \alpha_m)/R =$$
$$= f_{\mathcal{A}/R}(\alpha_1/R, \dots, \alpha_m/R) =$$

$$= f_{\mathcal{A}/R}(h(\alpha_1), \dots, h(\alpha_m)),$$

Donde m es el rango de la operación $f_{\mathcal{A}}$. Por consiguiente, h es un homomorfismo de álgebra $\mathcal{A}$ en álgebra cociente $\mathcal{A}/R$. ■

Nótese que el homomorfismo h definido con la ayuda de (1) se denomina homomorfismo natural del álgebra $\mathcal{A}$ en álgebra cociente $\mathcal{A}/R$.

TEOREMA 2.12. Sea h un homomorfismo de álgebra $\mathcal{A}$ en álgebra $\mathfrak{B}$ y R una tal relación binaria en $|\mathcal{A}|$ que para todos α, b de $|\mathcal{A}|$ se tenga

(1) $\alpha R b$ si solamente si $h(\alpha) = h(b)$.

En ese caso R es una congruencia en álgebra $\mathcal{A}$

Demostración. La relación R es una equivalencia de función h y, en virtud del TEOREMA 2.4.4, es una relación de equivalencia en $|\mathcal{A}|$.

Sea $f_{\mathcal{A}}$ una operación principal cualquiera (de rango m) del álgebra $\mathcal{A}$ y $f_{\mathfrak{B}}$ la operación principal correspondiente de álgebra $\mathfrak{B}$. En virtud de (1), para todos $a_1, b_1, \dots, a_m, b_m$ del conjunto $|\mathcal{A}|$ de

(2) $a_1 R b_1, \dots, a_m R b_m$

Se deducen las igualdades

(3) $h(a_1) = h(b_1), \dots, h(a_m) = h(b_m)$.

Supongamos que los elementos $a_1, b_1, \dots, a_m, b_m$ cumplen con las condiciones (2) y, también las condiciones (3). Ya que h es un momorfismo de $\mathcal{A}$ en $\mathcal{B}$, se tiene que

$$h\left(f_{\mathcal{A}}(a_1, \dots, a_m)\right) = f_{\mathcal{B}}\left(h(a_1), \dots, h(a_m)\right)$$

$$= f_{\mathcal{B}}\left(h(b_1), \dots, h(b_m)\right)$$

$$= h\left(f_{\mathcal{A}}(b_1, \dots, b_m)\right).$$

Así de (2) se deduce la igualdad

$$h\left(f_{\mathcal{A}}(a_1, \dots, a_m)\right) = h\left(f_{\mathcal{A}}(b_1, \dots, b_m)\right).$$

De allí, por la definición de R, viene

(4) $f_{\mathcal{A}}(a_1, \dots, a_m)\, R f_{\mathcal{A}}(b_1, \dots, b_m)$.

En resumen, para todos los elementos $a_1, b_1, \dots, a_m, b_m$ del conjunto $|\mathcal{A}|$ de (2) se deduce (4). Por consecuente, R es una congruencia en $\mathcal{A}$. ■

Ejercicios

1. Sean $+$, $\cdot$, operaciones ordinarias de adición y de multiplicación sobre el conjunto N de los números naturales y h la aplicación del conjunto N en N tal que $h(x) = 2^x$ para todo x de N. Demostrar que h es un homomorfismo del álgebra $\langle N, + \rangle$ en el álgebra $\langle N, \cdot \rangle$.

2. Sean $+$ y $\cdot$ las operaciones ordinarias de adicion y de multiplicación sobre el conjunto R de los números reales y a un numero real positivo fijo. Sea h la aplicación de R en R tal que $h\ (x) = \ a^x$ para todo x de R. Demostrar que h es un homomorfismo del álgebra $\langle R, + \rangle$ en el álgebra $\langle R,\ \cdot \rangle$.

3. Sea h un homomorfismo del álgebra $\langle A,\ f \rangle$ sobre el álgebra $\langle B,\ g \rangle$, donde f y g son operaciones binarias. Demostrar que:

(a) si la operación f es comutativa, la operación g lo es igualmente;

(b) si la operación f es asociativa, la operación g lo es igualmente;

(c) si e es un elemento neutro respecto a la operación $f, f\ (e)$ es un elemento neutro respecto a la operación g;

(d) si el elemento x es simétrico respecto a la operación f, el elemento $f\ (x)$ es simétrico relativamente a la operación g; si los elementos x y x' son mutuamente simétricos respecto a la operación f, los elementos $f\ (x)$ y $f\ (x')$ son mutuamente simétricas relativamente a la operación g.

4. Sean N el conjunto de los números naturales y $B = \{2^x | \ x \ \in N\}$. Sea h la aplicación del álgebra $\langle N, + \rangle$ sobre el álgebra $\langle B,\ \cdot \rangle$ tal que para todo x de N se verifica la igualdad $h\ (x) = \ 2^x$. Mostrar que h es un isomorfismo.

5. Sean R el conjunto de los números reales, R_+^* el conjunto de los números reales positivos, a un número real positivo distinto de uno. Sea h la aplicación del álgebra $\langle R, + \rangle$ en el álgebra $\langle R_+^*,\ \cdot \rangle$ tal que $h\ (x) = \ a^x$ para cada x de R. Demostrar que h es un isomorfismo.

6. Sean f un monomorfismo del álgebra $\mathcal{A}$ en $\mathcal{B}$ y g un monomorfismo del álgebra $\mathcal{B}$ en el álgebra $\mathcal{C}$. Demostrar que la composición $g \circ f$ es un monomorfismo del álgebra $\mathcal{A}$ en el álgebra $\mathcal{C}$.

7. Proporcionar un ejemplo de un álgebra $\mathcal{A}$ y de una relación de equivalencia R sobre $|\mathcal{A}|$ que no sea una congruencia en el álgebra $\mathcal{A}$.

8. Sea h un homomorfismo del álgebra $\mathcal{A}$ en el álgebra $\mathcal{B}$. Demostrar que el conjunto $Im\ |\mathcal{A}|$ (imagen homomorfa del conjunto base del álgebra $\mathcal{A}$) es cerrado en el álgebra $\mathcal{B}$.

9. Sea h un homomorfismo del álgebra $\mathcal{A}$ en el álgebra $\mathcal{B}$. Demostrar que el álgebra
$\langle \mathcal{C}, f_1 \mid \mathcal{C}, \dots, f_s \mid \mathcal{C} \rangle$,
Donde $\mathcal{C} = \ Im\ |\mathcal{A}|$, es una subálgebra del álgebra $\mathcal{B} = \ \langle \mathcal{B}, f_1, \dots, f_s \rangle$. Esta álgebra es llamada imagen homomorfa del álgebra $\mathcal{A}$ con homomorfismo h.

10. Sea h un homomorfismo del álgebra $\mathcal{A}$ en el álgebra $\mathcal{B}$. Demostrar que la imagen homomorfa del álgebra $\mathcal{A}$ con este homomorfismo es isomorfa al álgebra cociente $\mathcal{A}|\mathrm{R}$, donde R es una congruencia generada por el homomorfismo h.

11. Demostrar que todo homomorfismo h del álgebra $\mathcal{A}$ sobre el álgebra $\mathcal{B}$ es una composición del homomorfismo natural del álgebra $\mathcal{A}$ sobre su álgebra cociente y del isomorfismo de esta álgebra cociente sobre el álgebra $\mathcal{B}$.

§ 3. Grupos

Noción de grupo. Esta noción es un caso particular de álgebras que juegan un rol importante en matemáticas teóricas y aplicadas.

DEFINICIÓN. El álgebra $\mathcal{G} = \ \langle G,\ *,\ ' \rangle$ del tipo $(2, 1)$ se denomina *grupo* si sus operaciones principales cumplen con las condiciones (axiomas):

(1) La operación binaria $*$ es asociativa, es decir para todos los elementos a, b, c de $G\ a\ *\ (b\ *\ c) = \ (a\ *\ b)\ *\ c$;

(2) Existe en G un elemento neutro a la derecha respecto a la operación $*$, es decir un elemento e por el cual $a\ *\ e = \ a$ con a independientemente a de G;

(3) Para todo elemento a de G se tiene la igualdad $a\ *\ a' = e$.

Así, el grupo es un conjunto no vacío previsto de dos operaciones: una operación binaria $*$ y una operación unaria$'$. La operación binaria es asociativa y tiene un elemento neutro a la derecha, mientras que la operación unaria es una operación

de paso al elemento simétrico a la derecha respecto a la operación binaria y, por consiguiente cada elemento del grupo incluye un elemento simétrico a la derecha respecto a la operación binaria del grupo $*$.

DEFINICIÓN. Un grupo $\mathcal{G} = \langle G,\ *,\ ' \rangle$ se denomina *abeliano* o *conmutativo* si la operación binaria del grupo $*$ es conmutativa, es decir si para todos a, b de G $a * b = b * a$.

DEFINICIÓN. Se denomina *orden del grupo* $\mathcal{G} = \langle G,\ *,\ ' \rangle$ el número de elementos del conjunto base G del grupo cuando G es finito. Si G es un conjunto infinito, el grupo $\mathcal{G}$ se denomina *grupo de orden infinito.*

Estudiando los grupos, generalmente se utiliza para las operaciones principales del grupo notaciones aditivas o multiplicativas. Con la utilización de la *notación multiplicativa* la operación binaria del grupo se denomina *multiplicación* y se escribe $a \cdot b$ (o ab) en lugar de $a * b$ denominando el elemento $a \cdot b$ el producto de los elementos a y b. El elemento simétrico de a denotado a^{-1} se denomina inverso del elemento a. El elemento neutro respecto a la multiplicación se denota e, 1 o $1_{\mathcal{G}}$ y se denomina *elemento idéntico o unidad del grupo.* En la notación multiplicativa la definición antes mencionada de grupo se enuncia de la siguiente manera.

El álgebra $\mathcal{G} =< G,\ \cdot,\ \ ^{-1} >$ del tipo $(2, 1)$ se denomina grupo si sus operaciones principales cumplen con las condiciones siguientes:

(1) La operación binaria $\cdot$ es asociativa, es decir para todos los elementos a, b, c de G se verifica la igualdad $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(2) Existe en G una unidad a la derecha, es decir un elemento e tal que $a \cdot e = a$ para todo elemento a de G;
(3) Para todo elemento a de G se tiene la igualdad $a \cdot a^{-1} = e$.

La noción de potencia natural a^n del elemento a de un grupo multiplicativo $< G,\ \cdot,\ \ ^{-1} >$ se define de la manera siguiente:

$a^0 = e$, $\ a^n = a \cdot a \ldots a$ para $n \in \mathrm{N} \setminus \{0\}$.

En una notación aditiva la operación binaria del grupo se denomina adición y se escribe $a + b$ en vez de $a * b$ llamando al elemento $a + b$ suma de los elementos a y b. El elemento simétrico del elemento a se denota $(-a)$ y se denomina elemento opuesto de a. El elemento neutro por otro lado se designa por el símbolo 0 o $0_{\mathcal{G}}$ y se denomina elemento cero o cero del grupo. En escritura aditiva la definición del grupo se formula de la manera siguiente.

El álgebra $\mathcal{G} = \langle G,\ +,\ - \rangle$ del tipo $(2, 1)$ se denomina grupo si sus operaciones principales cumplen con las condiciones siguientes:

(1) La operación binaria $+$ es asociativa, es decir que para los elementos a, b, c de G se tiene que $a + (b + c) = (a + b) + c$;
(2) Existe en G un cero a la derecha, es decir un elemento 0 tal que $a + 0 = a$ para todo elemento a de G;
(3) Para todo elemento a de G $a + (-a) = 0$.

Ejemplos de grupos. 1. Sea $\boldsymbol{Q}$ el conjunto de todos los números racionales con la adición ordinaria y una operación unaria $-$, operación de paso del número a al número opuesto $(-a)$. El álgebra $Q = \langle \boldsymbol{Q},\ +,\ - \rangle$ del tipo $(2, 1)$ es un grupo. Se conoce como *grupo aditivo de los números racionales*.

2. Sea $\boldsymbol{Q}^*$ el conjunto de todos los números racionales distintos de cero con la multiplicación ordinaria y operación unaria $^{-1}$, operación de paso del número a al número inverso a^{-1}. El álgebra $Q^* = \langle \boldsymbol{Q}^*,\ \cdot,\ \ ^{-1} \rangle$ es un grupo. Este grupo se denomina *grupo multiplicativo de los números racionales*.

3. Sean $\boldsymbol{R}$ el conjunto de todos los números reales con adición ordinaria y operación unaria que asocia a cada número real r el número opuesto $-r$. El álgebra $\mathcal{R}_+ = \langle \boldsymbol{R},\ +,\ - \rangle$ es un grupo. Se denomina *grupo aditivo de los números reales.*

4. Sean $\boldsymbol{R}^*$ el conjunto de todos los números reales distintos de cero con la multiplicación ordinaria y operación unaria $^{-1}$ que se asocia a cada número r diferente de cero su inverso r^{-1}. El álgebra $\mathcal{R}^* = \langle \boldsymbol{R}^*, \cdot, {}^{-1} \rangle$ es un grupo. Este grupo se denomina grupo multiplicativo de los números reales.

5. Sea S_n una colección de todas las permutaciones del conjunto $M = \{1, \dots, n\}$, es decir una colección de aplicaciones inyectivas de este conjunto sobre el mismo. Sean $\mathcal{S}_n = \langle S_n, \circ, {}^{-1} \rangle$ un álgebra con una operación binaria $\circ$ (composición de aplicaciones) y una operación unaria $^{-1}$ que asocia a la función f de S_n a su función inversa f^{-1}. Esta álgebra es un grupo. De hecho, siguiendo el TEOREMA 2.3.10 una composición de dos permutaciones cualesquiera del conjunto M es una permutación de este conjunto. Según el TEOREMA 2.3.5 una composición de permutaciones es asociativa. Una permutación idéntica i_M es un elemento neutro respecto a la composición de permutaciones. Para toda permutación f del conjunto M $f \circ f^{-1} = i_M$. Este grupo se denomina *grupo simétrico de las permutaciones de índice* n; que tiene el orden $n!$ y que no es conmutativo para $n > 2$.

6. Sea G el conjunto de todos los vectores de un plano dado con la operación ordinaria $+$ de la adicion de los vectores y la operación unaria $-$ que asocia a cada vector v a su opuesto $(-v)$. El álgebra $\langle G, +, - \rangle$ es un grupo. Este grupo se denomina *grupo aditivo de los vectores del plano.*

7. Consideremos el conjunto G de todas las rotaciones del plano alrededor de un punto dado 0. Una rotación del plano se asimila a una transformación del plano, es decir a una aplicación inyectiva del plano sobre el mismo. Dos rotaciones de ángulos α y β se denomina congruentes si $\alpha - \beta = 2n\pi$, donde n es un entero. La composición $\varphi \circ \psi$ de dos rotaciones ψ y φ respectivamente de los angulos α y β es una rotación de ángulo $\alpha + \beta$. Si ψ es una rotación de ángulo α, ψ^{-1} es una rotación de Angulo $(-\propto)$. El álgebra $\langle G, \circ, {}^{-1} \rangle$ es un grupo. Se denomina *grupo de rotación del plano* alrededor del punto dado.

8. Sea H_n un conjunto compuesto de n rotaciones de un plano dado de ángulos $\frac{2k\pi}{n}$, $k = 0, 1, \dots, n-1$, alrededor de un punto O fijo, que constituye una aplicación de un polígono regular en n angulos de centro al punto O sobre el mismo. El álgebra $\langle H_n, \circ, {}^{-1} \rangle$ es un grupo. Se denomina *grupo de rotación de un polígono regular en* n *angulos*.

9. Consideremos un conjunto G de todas las rotaciones de un espacio alrededor del punto O, que constituye una aplicación de un cuerpo regular dado (tetraedro, cubo, icosaedro, dodecaedro) de centro al punto O sobre el mismo. El álgebra $\langle G, \circ, {}^{-1} \rangle$ es un grupo. Se denomina *grupo de rotaciones (auto congruente) del cuerpo regular dado.*

Propiedades elementales del grupo. Se utilizará más adelante la notación multiplicativa para las operaciones del grupo.

PROPIEDAD 3.1. Para todo elemento a del grupo $a^{-1}a = e$, es decir el *inverso a la derecha de* a *es igualmente un inverso a la izquierda*.

Demostración. Del segundo y del tercer axioma del grupo se deduce que:

$a^{-1} = a^{-1}e = a^{-1}(aa^{-1}) = (a^{-1}a)\, a^{-1}$.

En virtud de los axiomas del grupo se deducen las igualdades

$$a^{-1}a = (a^{-1}a)\, e = (a^{-1}a)\, (a^{-1}(a^{-1})^{-1}) = \left((a^{-1}a)\, a^{-1}\right) (a^{-1})^{-1} =$$
$$= a^{-1}\, (a^{-1})^{-1} = e, \text{ es decir } a^{-1}a = e. \ \blacksquare$$

PROPIEDAD 3.2. *Para cada elemento* a *del grupo, el elemento* a^{-1} *es el único elemento inverso. Cada elemento* a *del grupo posee un elemento inverso único a la derecha y un elemento inverso único a la izquierda, los dos que coinciden con* a^{-1}.

Esta propiedad resulta directamente de la definición del elemento inverso, de la propiedad 3.1, del TEOREMA 1.4 y del corolario 1.5 de este último.

PROPIEDAD 3.3. *Para todo elemento* a *del grupo* $ea = a$, *es decir que la unidad a la derecha es igualmente una unidad a la izquierda.*

Demostración. A partir de los axiomas del grupo y de la propiedad 3.1 se deduce que

$ea = aa^{-1}\, a = a\,(a^{-1}a) = ae = a$, es decir $ea = a$. ■

POPIEDAD 3.4. *El elemento e del grupo es el único elemento unidad del grupo. Es decir el único elemento unidad a la derecha y unidad a la izquierda del grupo.*

Esta propiedad se deduce directamente de la definición de los elementos unidades, de la propiedad 3.3, del TEOREMA 1.1 y del corolario 1.2 de este último.

PROPIEDAD 3.5. *Para todos los elementos a, b del grupo cada una de las ecuaciones $ax = b$ y $ya = b$ respecto a las variables x e y poseen una solución única en el grupo.*

Demostración. El elemento $a^{-1}b$ es la solución de la ecuación $ax = b$, *puesto que* $a\,(a^{-1}b) = (aa^{-1})b = eb = b$. Por otro lado, si c es una solución arbitraria de la ecuación $ax = b$, se tiene que $c = ec = (a^{-1}a)\,c = a^{-1}\,(ac) = a^{-1}b$. Por consiguiente, el elemento $a^{-1}b$ es la única solución de la primera ecuación. Se demuestra de manera análoga que el elemento ba^{-1} es la única solución de la segunda ecuación. ■

Propiedad 3.6 (regla de simplificación). Para todos los elementos a, b, c del grupo $ac = bc$ se deduce que $a = b$ y de $ca = cb$ $a = b$.

Demostración. Si $ac = bc$, a y b son las soluciones de la ecuación $yc = bc$. De la propiedad 3.3 deducimos que a = b. Se prueba de manera análoga que de $ca = cb$ se deduce que $a = b$. □

Propiedad 3.7. Para todos los elementos a, b, c del grupo se deduce de $ab = a$ que $b = e$ y de $ca = a$ que $c = e$.

Demonstracion. Si $ab = a$, se tiene $ab = ae$. De acuerdo con la regla de simplificación de $ab = ae$ se deduce que $b = e$. Análogamente $ca = a$ se deduce que $ca = ea$ y $c = e$. □

Propiedad 3.8. EL elemento a es en el grupo el inverso de Sea a un elemento del grupo inverso a^{-1}, es decir que a^{-1} es $(a^{-1})^{-1} = a$.

Demostración. De acuerdo con el tercer axioma de grupo $(a^{-1})(a^{-1})^{-1} = e$. Por la propiedad 3.1 $a^{-1}a = e$. Por lo tanto, $a^{-1}(a^{-1})^{-1} = a^{-1}a$. De acuerdo con la regla de simplificación se deduce la igualdad $(a^{-1})^{-1} = a$. ■

Propiedad 3.9. Para todos los elementos a, b del grupo de $ab = e$ se deduce que $b = a^{-1}$ y $a = b^{-1}$.

Esta propiedad se deduce directamente de la definición del elemento inverso y la propiedad 3.2.

Homomorfismos de grupos. De acuerdo con la definición de los homomorfismos de las álgebras así como el hecho de que los grupos son un caso especial de álgebras, formulamos las siguientes DEFINICIONES.

Sean $\mathcal{G} = \langle G, \cdot, {}^{-1}\rangle$ y $\mathcal{H} = \langle H, \circ, {}^{-1}\rangle$ grupos multiplicativos.

Se dice que la aplicación h del conjunto G en H respecto a las operaciones principales del grupo $\mathcal{G}$ si se cumplen las condiciones:

(1) $h\,(ab) = h\,(a) \circ h\,(b)$ para todos a, b de G;

(2) $h\,(a^{-1}) = (h\,(a))^{-1}$ para todo a de G.

Definición. Se denomina *homomorfismo* de un grupo $\mathcal{G}$ en (sobre) el grupo $\mathcal{H}$ a toda aplicación del conjunto G en (sobre) H que respeta las operaciones principales del grupo $\mathcal{G}$. El homomorfismo del grupo $\mathcal{G}$ sobre $\mathcal{H}$ se denomina epimorfismo.

Definición: Se denomina isomorfismo a todo homomorfismo h del grupo $\mathcal{G}$ sobre el grupo $\mathcal{H}$ si h es una aplicación inyectiva del conjunto G sobre H. Los grupos $\mathcal{G}$ y $\mathcal{H}$ son llamados isomorfos si existe un isomorfismo del grupo $\mathcal{G}$ sobre$\mathcal{H}$.

La notación $\mathcal{G} \cong \mathcal{H}$ significa que los grupos $\mathcal{G}$ *y* $\mathcal{H}$ son isomorfos.

Definición. Se denomina *monomorfismo* o *inyección* al homomorfismo h del grupo $\mathcal{G}$ en el grupo $\mathcal{H}$ si h es una aplicación inyectiva del conjunto G en H.

DEFINICIÓN. Se denomina *endomorfismo del grupo* $\mathcal{G}$ al homomorfismo de $\mathcal{G}$ en el mismo. El isomorfismo de $\mathcal{G}$ sobre el mismo se denomina *automorfismo del grupo* $\mathcal{G}$.

Mientras que, por ejemplo, es un automorfismo es la aplicación identidad del grupo sobre el mismo.

TEOREMA 3.1. Si la aplicación h del grupo $\mathcal{G} = < G, \cdot, \ ^{-1} >$ en el grupo $\mathcal{H} = < H, \circ, \ ^{-1} >$ respecto a la operación binaria del grupo $\mathcal{G}$, es decir si

(1) $h\,(ab) = h\,(a) \circ h\,(b)$ para todos a, b de G,

ahora bien h transforma la unidad del grupo $\mathcal{G}$ en la unidad del grupo $\mathcal{H}$ y constituye un homomorfismo.

Demostración. Sean e la unidad del grupo $\mathcal{G}$ y $e' = h\,(e)$. En virtud de (1), $h\,(e \cdot e) = h\,(e) \circ h\,(e) = h\,(e)$, es decir que $e' \circ e' = e'$. Según la propiedad 3.7, se deduce que e' es una unidad del grupo$\mathcal{H}$.

Sea a un elemento cualquiera del grupo $\mathcal{G}$. En virtud de (1), de $a * a^{-1} = e$ se deduce que $h\,(a) \circ h\,(a^{-1}) = e'$. Según la propiedad 3.9 se obtiene

(2) $h\,(a^{-1}) = (h\,(a))^{-1}$ para todo a de G.

Sobre la base de (1) y (2) se concluye que h es un homomorfismo del grupo $\mathcal{G}$ en$\mathcal{H}$. ■

TEOREMA 3.2. Sobre un conjunto de grupos cualesquiera la relación de isomorfismo es reflexiva, transitiva y simétrica, es decir es una relación de equivalencia.

Este TEOREMA se deriva directamente del TEOREMA 2.5.

Ejemplos. 1. Consideremos el conjunto Q^* de todos los números racionales distintos de cero y $\mathcal{Q}^* = < Q^*, \cdot, \ ^{-1} >$ constituye un grupo multiplicativo de números racionales. Sean Q_+ el conjunto de todos los números racionales positivos y $Q_+ = < Q_+, \cdot, \ ^{-1} >$ un grupo multiplicativo de los números racionales positivos. La aplicación h del conjunto Q^* sobre Q_+ definido por la formula $h\,(a) = |a|$ para cada a de Q^*, donde $|a|$ es el valor absoluto del numero a, respecto a las operaciones principales del grupo Q^*. De hecho, para todos a, b de Q^* se cumplen las igualdades $|ab| = |a| \ |b|$ y $|a^{-1}| = |a|^{-1}$. Por consiguiente, la aplicación h es un homomorfismo del grupo $\mathcal{Q}^*$ sobre $\mathcal{Q}_+$.

2. Consideremos el conjunto R_+ de todos los números reales positivos y $\mathcal{R}_+ = < R_+, \cdot, \ ^{-1} >$ constituye un grupo multiplicativo de los números reales positivos. Sean R el conjunto de todos los números reales y $\mathcal{R} = < R, +, - >$ el grupo aditivo de números reales. Véase la aplicación $f: R_+ \to R$ definida por la formula $f\,(x) = \log x$. La función f es una aplicación inyectiva del conjunto R_+ sobre R que respeta las operaciones principales del grupo $\mathcal{R}_+$. De hecho para todos x, y de $R_+ \log\,(xy) = \log x + \log y$, $\log(x^{-1}) = -\log x$.

Por consiguiente, f es un isomorfismo del grupo $\mathcal{R}_+$ sobre el grupo $\mathcal{R}$.

3. consideremos la aplicación g del conjunto R sobre R_+ definida por la formula $g\,(x) = 2^x$. La aplicación g es una aplicación inyectiva de R sobre R_+ y ella respeta las operaciones principales del grupo aditivo $\mathcal{R} = < R, +, - >$, ya que $2^{x+y} = 2^x 2^y$ y $2^{-x} = (2x)^{-1}$. Por lo tanto, g es un isomorfismo del grupo aditivo $\mathcal{R}$ sobre el grupo multiplicativo $R_+ = < R, \cdot, \ ^{-1} >$.

Subgrupos. Consideremos al grupo $\mathcal{G} = < G, \cdot, \ ^{-1} >$.

DEFINICIÓN. Se denomina subgrupo del grupo $\mathcal{G}$ a toda subálgebra de este grupo.

De manera más detallada, en función de la definición de sub-álgebra, la definición de subgrupo puede ser enunciada de la siguiente manera.

El álgebra $\mathcal{H} = < H, \odot, \ ^{-1} >$ del tipo $(2, 1)$ es llamada *subgrupo del grupo* $\mathcal{G} = < G, \cdot, \ ^{-1})$ si $H \subset G$ y si la aplicación identidad del conjunto H en G es un monomorfismo del álgebra $\mathcal{H}$ en $\mathcal{G}$, es decir, si se cumplen las condiciones:

(1) $a \odot b = a \cdot b$ para todos a, b de H;

(2) $a^{-1} = a^{-1}$ para todo a de H.

La notación $\mathcal{H} \ \text{-3} \ \mathcal{G}$ significa que el álgebra $\mathcal{H}$ es un subgrupo del grupo $\mathcal{G}$.

Si $\mathcal{H} \ \text{-3} \ \mathcal{G}$, de la definición de subgrupo se deduce que el conjunto H es cerrado en el grupo $\mathcal{G}$ y, por lo tanto, la aplicación de toda operación principal del grupo $\mathcal{G}$ en los elementos de H resulta de nuevo un elemento de H. Además, en virtud de

las condiciones (1) y (2) cada una de las operaciones principales del álgebra $\mathcal{H}$ es una restricción de la operación principal correspondiente del grupo $\mathcal{G}$ al conjunto H.

TEOREMA 3.3. *Todo subgrupo del grupo es un grupo. El elemento neutro del grupo es el elemento neutro de cualquiera de sus subgrupos.*

Demostración. Sean $\mathcal{H} = < H, \odot, \quad ^{-1} >$ un subgrupo del grupo multiplicativo $\mathcal{G} = < G, \cdot, \quad ^{-1} >$ y e el elemento neutro del grupo $\mathcal{G}$.

La operación binaria $\odot$ del álgebra $\mathcal{H}$ es asociativa, puesto que, en virtud de (1), para todos a, b, c de H, se tiene

$$a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c.$$

El elemento e pertenece a H, ya que, en virtud de (1) Y (2), para todo a de H, se tiene que $e = a \cdot a^{-1} = a \odot a^{-1} \subset H$.

En virtud de (1), para todo a de H se obtiene $a \odot e = a \cdot e = a$, es decir que e es un elemento neutro a la derecha respecto a la operación$\odot$.

En virtud de (2), para todo a de H se obtiene $a \odot a^{-1} = a \cdot a^{-1} = e$, es decir que $a \odot a^{-1} = e$. Por consiguiente, el álgebra $\mathcal{H}$ es un grupo y e es su elemento neutro. ■

Sean $\mathcal{G} = < G, \cdot, \quad ^{-1} >$, un conjunto multiplicativo y A un subconjunto no vacio del conjunto G cerrado respecto a las operaciones principales del grupo $\mathcal{G}$. Sean $\odot$ y $^{-1}$ las restricciones de las operaciones principales del grupo $\mathcal{G}$ en el conjunto A, dicho de otro modo

$a \odot b = a \cdot b$ para todos a, b de A;

$a^{-1} = a^{-1}$ para todo a de A.

Mientras que, se deduce del TEOREMA 2.6 y 3.3 el álgebra

(3) $\mathcal{A} = < A, \odot, \quad ^{-1} >$

Es un subgrupo del grupo $\mathcal{G}$. Por lo tanto, el grupo $\mathcal{A}$ del grupo $\mathcal{G}$ es definido de manera inequívoca por el subconjunto no vacío A cerrado en $\mathcal{G}$. Tambien en lugar de la notación (3) se escribe: << subgrupo $\mathcal{A} = < A, \cdot, \quad ^{-1} > \gg$ y se lee: << el conjunto A es un subgrupo del grupo $\mathcal{G}$ respecto a las operaciones $\cdot$ y $^{-1}$ >>.

TEOREMA 3.4. *La relación binaria (<< es un subgrupo>>) sobre el conjunto de subgrupos del grupo dado es reflexivo, transitivo, y antisimetrico y, por lo tanto, es una relación de orden no estricto.*

Este TEOREMA es un caso especial del TEOREMA 2.8.

TEOREMA 3.5. *Una intersección de una colección arbitraria (no vacía) de subgrupos del grupo $\mathcal{G}$ es un sub-grupo del grupo $\mathcal{G}$.*

Este TEOREMA se realiza directamente del TEOREMA 3.3.

Se deduce del TEOREMA 3.6 que para todo conjunto M de elementos del grupo $\mathcal{G}$ existe un subgrupo minimal $\mathcal{H}$ que contiene M. Es fácil de ver que $\mathcal{H}$ es una intersección de todos los subgrupos del grupo $\mathcal{G}$ que contienen a M. Este subgrupo minimal $\mathcal{H}$ se denomina *subgrupo generado por el conjunto M,* mientas que M se denomina *conjunto de generatrices* o *sistema de generatrices del grupo $\mathcal{H}$*.

DEFINICIÓN. Un grupo es dicho *cíclico* si es generado por un solo elemento (conjunto de un elemento).

Ejemplos. 1. Consideremos un grupo aditivo $R_+ = < R, +, -> $ de los números reales. El conjunto Q de los números racionales es un sub-grupo del conjunto R que es cerrado en las operaciones principales del grupo $\mathcal{R}_+$. Por lo tanto, el álgebra $\mathcal{Q} =< Q, +, ->$, grupo aditivo de los números racionales, es un subgrupo del grupo $\mathcal{R}_+$.

2. Consideremos un grupo multiplicativo $\mathcal{R}^* = < R^*, \cdot, \quad ^{-1} >$ de los números reales. El conjunto Q^* de los números racionales diferentes de cero es un sub-grupo del conjunto R^* cerrado en las operaciones principales del grupo $\mathcal{R}^*$. Por lo tanto, el álgebra $\mathcal{Q}^* = < Q^*, \cdot, \quad ^{-1} >$, grupo multiplicativo de los números racionales, es un sub-grupo del grupo $\mathcal{R}^*$.

3. Sean $\mathcal{G} = < G, \cdot, \quad ^{-1} >$ un grupo de rotaciones del plano alrededor del punto dado O y H_n un conjunto compuesto de n rotaciones del plano alrededor del punto O que constituye una aplicación de un polígono regular de n ángulos de centro

O sobre el mismo. El conjunto H_n es cerrado respecto a las operaciones principales del grupo $\mathcal{G}$. Por lo tanto, el álgebra $\mathcal{H}_n = < H_n, \circ, \ ^{-1} >$, grupo de rotaciones de un polígono regular de n ángulos, es un subgrupo del grupo $\mathcal{G}$.

Ejercicios

1. Decir si los conjuntos de números racionales siguientes son cerrados respecto a las operaciones principales del grupo aditivo de los números racionales:
   (a) El conjunto de todos los enteros;
   (b) El conjunto de todos los números naturales;
   (c) El conjunto de todos los enteros pares;
   (d) El conjunto de todos los enteros múltiplos del entero dado n;
   (e) El conjunto de todos los enteros impares;
   (f) El conjunto de todos los números racionales con denominadores impares;
   (g) El conjunto de todos los números racionales con denominadores pares,
2. Decir si los conjuntos de números racionales siguientes son cerrados respecto a las operaciones principales del grupo multiplicativo de los números racionales:
   (a) El conjunto $(1, -1)$;
   (b) El conjunto de todos los números distintos de cero con denominadores pares;
   (c) El conjunto de todos los números racionales distintos de cero con denominadores impares;
   (d) El conjunto de todos las potencias enteras del numero 2;
   (e) El conjunto $\{p^n \mid n \text{ entero}\}$, donde p es un número primo.
3. Formar la tabla de multiplicación para los elementos de los siguientes grupos:
   (a) El grupo de rotaciones de un triángulo equilátero;
   (b) El grupo de rotaciones de un cuadrado;
   (c) El grupo de rotaciones de un pentágono regular;
   (d) El grupo aditivo de las clases residuales módulo 5;
   (e) El grupo multiplicativo de las clases residuales módulo 5, que forman los números primos con 5;
   (f) El grupo de todas las simetrías del rombo;
   (g) El grupo de todas las simetrías de un triángulo equilátero;
   (h) El grupo simétrico de las permutaciones de tercer grado;
   (i) El grupo de las simetrías de un rectángulo que no sea un cuadrado;
   (j) El grupo de todas las simetrías de un cuadrado.
4. Demostrar por recurrencia que el orden del grupo simétrico de las permutaciones de grado n es $n!$
5. Demostrar si $a^2 = e$ (siendo e el elemento unidad del grupo) para todo elemento a del grupo multiplicativo, entonces el grupo es abeliano.
6. Sean, g y h los elementos del grupo multiplicativo $\mathcal{G}$. Definamos la potencia de exponente negativo: $a^{-n} = (a^{-1})^n$. Demostrar que para todos los números m y n:
   (a) $(g^{-1})^n = (g^n)^{-1}$;
   (b) $g^m g^n = g^{m+n}$;
   (c) $(g^m)^n = g^{mn}$;
   (d) $(g \cdot h)^m = g^m \cdot h^m$ si $\mathcal{G}$ es un grupo abeliano.
7. Demostrar que todo grupo de cuatro o menos elementos es un grupo abeliano.
8. Mostrar que todo grupo de tres elementos es cíclico. Demostrar que para cualesquiera dos grupos de tres elementos cada uno son isomorfos.
9. Sean $\mathcal{G}$ un grupo abeliano aditivo y n un entero. Demostrar que la aplicación $x \longmapsto nx$ es un endomorfismo del grupo $\mathcal{G}$.
10. Mostrar que la aplicación $x \longmapsto 3^x$ es un isomorfismo del grupo aditivo de los números reales sobre un grupo multiplicativo de los números reales positivos.
11. Demostrar que el grupo simétrico de las permutaciones de tres elementos es isomorfo en el grupo de simetrías del triángulo equilátero.
12. Demostrar que el grupo de rotaciones del cuadrado no es isomorfo en el grupo de simetrías del rombo.
13. Considere un grupo abeliano multiplicativo $\mathcal{G}$. Mostrar que la aplicación $x \longmapsto x^{-1}$ es un automorfismo del grupo $\mathcal{G}$.

14. Demostrar que el grupo de simetrías de un tetraedro regular es isomorfo al grupo simétrico de las permutaciones de cuatro elementos.

15. Demostrar que un álgebra isomorfa a un grupo es un grupo.

§ 4. Anillos

Noción de anillo. Los anillos como los grupos son un caso particularmente importante de las álgebras.

DEFINICIÓN. Se denomina *anillo* a un álgebra $\mathcal{K} =< K,\ +,\ -,\ \cdot,\ 1 >$ del tipo $(2, 1, 2, 0)$ del cual las operaciones principales cumplen con las siguientes condiciones:

(1) El álgebra $< K,\ +,\ - >$ es un grupo abeliano;

(2) El álgebra $< K,\ \cdot,\ 1 >$ es un monoide;

(3) La multiplicación es distributiva respecto a la adición, es decir, para todos los elementos a, b, c de K
$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad c \cdot (a + b) = c \cdot a + c \cdot b.$

El conjunto base K del anillo $\mathcal{K}$ es igualmente denotado $|\mathcal{K}|$. Los elementos del conjunto K son llamados *elementos del anillo* $\mathcal{K}$.

DEFINICIÓN. El grupo $< K,\ +,\ - >$ se denomina grupo aditivo del anillo $\mathcal{K}$. El cero de este grupo, es decir, el *elemento neutro* respecto a la adición, se denomina cero del anillo y es denotado 0 o $0_{\mathcal{K}}$.

DEFINICIÓN. Un monoide $< K,\ \cdot,\ 1 >$ se denomina *monoide multiplicativo del anillo* $\mathcal{K}$. El elemento 1 denotado igualmente $1_{\mathcal{K}}$ constituye un elemento neutro respecto a la multiplicación se denomina unidad del anillo $\mathcal{K}$.

El anillo $\mathcal{K}$ es dicho commutativo si $a \cdot b = b \cdot a$ para todos los elementos a, b del anillo. El anillo $\mathcal{K}$ es dicho nulo si $|\mathcal{K}| = \{0_{\mathcal{K}}\}$.

DEFINICIÓN. Un anillo $\mathcal{K}$ se denomina *dominio de integridad* si es conmutativo, $0_{\mathcal{K}} \neq 1_{\mathcal{K}}$ y para todos $a, b \in K$ de $a \cdot b = 0$ se deduce $a = 0$ o $b = 0$.

DEFINICIÓN. Los elementos a y b del anillo $\mathcal{K}$ son llamados *divisores de cero* si $a \neq 0,\ b \neq 0$ y $ab = 0$ o $ba = 0$.

Remarquemos que todo dominio de integridad no tiene divisores de cero.

Ejemplos. 1. Sea Q el conjunto de todos los números racionales y

$Q[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in Q\}$.

El álgebra

$\mathcal{Q}[\sqrt{2}] =< Q\ [\sqrt{2}], +,\ -,\ \cdot,\ 1 >$

Del tipo $(2, 1, 2, 0)$, donde $+,\ \cdot$ son las operaciones ordinarias de adición y de multiplicación de números reales y – una operación unaria del paso del número dado a su opuesto, es un anillo conmutativo.

2. Consideremos un conjunto K de todas las funciones reales definidas sobre el conjunto R de los números reales. La suma $f + g$, el producto $f \cdot g$, la función $-f$ y la función unaria 1 se definen habitualmente, a saber:

$(f\ +\ g)\ (x)\ =\ f\ (x)\ +\ g\ (x);$

$(f \cdot g)\ (x) = f\ (x) \cdot g(x);$

$(-f)(x) =\ -f\ (x);$

$1\ (x)\ =\ 1.$

Una verificación directa muestra que el álgebra $< K, +,\ -,\ \cdot,\ 1 >$ es un anillo conmutativo.

3. Consideremos un anillo cualquiera $\mathcal{K} =< K, +,\ -,\ \cdot,\ 1 >$.

La tabla de la forma

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$,

Donde a, b, c, d son elementos de K, y es llamada *matriz cuadrada* de orden dos sobre $\mathcal{K}$ o matriz 2×2 sobre $\mathcal{K}$. El conjunto de todas las matrices 2×2 sobre $\mathcal{K}$ será denotado $K^{2\times 2}$. Introduzcamos sobre este conjunto la relación de igualdad. Las matrices

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ y $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$

Son dichas iguales y se escribe

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$

Si $a = e,\ b = f,\ c = g,\ d = h.$

Las matrices

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ y $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Son llamadas matriz unidad y matriz nula respectivamente. En el conjunto de matrices 2×2 sobre $\mathcal{K}$, las operaciones de adición, multiplicación y la operación unaria son definidas de la siguiente manera:

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a + a_1 & b + b_1 \\ c + c_1 & d + d_1 \end{bmatrix}$;

$-\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$;

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} aa_1 + bc_1 & ab_1 + bd_1 \\ ca_1 + dc_1 & cb_1 + dd_1 \end{bmatrix}$.

Se verifica directamente que el álgebra $< K^{2\times 2}, +, - >$ es un grupo abeliano, el álgebra $< K^{2\times 2},\ \cdot,\ I >$ un monoide y el producto de las matrices es ditributivo respecto a la adicion. Por consiguiente, el álgebra $< K^{2\times 2},\ +,\ -,\ \cdot,\ I >$ es un anillo que ademas no es conmutativo. Este anillo se denomina *anillo de las matrices* $2\ \times 2$ sobre $\mathcal{K}$ y se le designa por el símbolo $\mathcal{K}^{2\times 2}$.

Propiedades elementales del anillo. Sea $\mathcal{K}$ un anillo. Puesto que el álgebra $< K,\ +, - >$ es un grupo abeliano, en virtud de la propiedad 3.5 para todos los elementos $a, b, (-b)$ notados igualmente $a - b$.

TEOREMA 4.1. Sea $\mathcal{K} = <\mathrm{K}, +,\ -,\ \cdot,\ 1>$ *un anillo. Ahora bien para todos los elementos* a, b, c *del anillo:*

(1) Si $a\ +\ b\ =\ a$, se tiene $b\ =\ 0$;
(2) Si $a\ +\ b\ =\ 0$, se tiene $b\ =\ -a$;
(3) $-\ (-a)\ =\ a$;
(4) $0 \cdot a = a \cdot 0 = 0$;
(5) $(-a)\ b = a\ (-b) =\ -(ab)$;
(6) $(-a)(-b) = a \cdot b$;
(7) $(a - b)c = ac - bc$ y $c\ (a - b) = ca - cb$.

Demostración. (1) si $a\ +\ b\ =\ a$, se tiene $b = 0 + b = (-a + a) + b =\ -a + (a + b) =\ -a + a = 0$.

(2) Si $a\ +\ b\ =\ 0$, se obtiene

$b = 0 + b = (-a + a) + b =\ -a + (a + b) =\ -a + 0 =\ -a$.

(3) En el grupo aditivo de un anillo $(-a) + \big(-(-a)\big) =\ -a + a$. De donde, en virtud de la regla de simplificación, se deduce la igualdad $-\ (-a) = a$.

(4) En virtud de la distribución de la multiplicación respecto a la adición $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$. En virtud de (1) de la ultima igualdad se deduce $0 \cdot a = 0$.

(5) En virtud de (4) y de la distributividad de la multiplicación respecto a la adición $ab + (-a)\, b = \big(a + (-a)\big)\, b = 0$, es decir $ab + (-a)\, b = 0$. De donde, en virtud de (2), se deduce que $(-a)\, b = -(ab)$. De manera análoga se demuestra que $a\,(-b) = -(ab)$.

(6) En virtud de (5) y (3) $\quad (-a)\cdot(-b) = -\big((-a)\cdot b\big) = -(-(ab)) = a\cdot b$.

(7) En virtud de (5) y de la distributividad de la multiplicación respecto a la adición $(a-b)\cdot c = \big(a + (-b)\big)\cdot c = a\cdot c + (-b)\times c = a\cdot c + (-b\cdot c) = a\cdot c - b\cdot c$. ■

Homomorfismos de anillos. De acuerdo con la definición de homomorfismo de álgebras y al respecto con el hecho que los anillos son un caso particular de álgebras enunciamos las siguientes DEFINICIÓN.

Sean $\mathcal{K} = \langle K, +, -, \circ, 1\rangle$ y $\mathcal{K}' = < K', +, -, \cdot, 1' >$ anillos. Se dice que la aplicación h del conjunto K en K' respeta las operaciones principales del anillo $\mathcal{K}$ si se cumplen las condiciones:

(1) $h\,(a + b) = h\,(a) + h\,(b)$ para todos a, b de K;

(2) $h\,(-a) = -h\,(a)$ para todo a de K;

(3) $h\,(a\cdot b) = h\,(a)\circ h\,(b)$ para todos a, b de K;

(4) $h\,(1) = 1'$.

DEFINICIÓN. Se denomina *homomorfismo del anillo $\mathcal{K}$ en (sobre) el anillo $\mathcal{K}'$ a* la aplicación del conjunto K en (sobre) K' que respeta todas las operaciones principales del anillo $\mathcal{K}$. Un homomorfismo del anillo $\mathcal{K}$ sobre $\mathcal{K}'$ es nombrado *epimorfismo.*

DEFINICIÓN. Se denomina *isomorfismo* al homomorfismo h del anillo $\mathcal{K}$ sobre el anillo $\mathcal{K}'$ si h es una aplicación inyectica del conjunto k sobre K'. Los anillos $\mathcal{K}$ y $\mathcal{K}'$ son dichos *isomorfos* si existe un isomorfismo del anillo $\mathcal{K}$ sobre $\mathcal{K}'$.

La notación $\mathcal{K} \cong \mathcal{K}'$ significa que el anillo $\mathcal{K}$ y $\mathcal{K}'$son isomorfos.

DEFINICIÓN. Se denomina *monomorfismo* o *inyección* al homomorfismo h del anillo $\mathcal{K}$ en el anillo $\mathcal{K}'$ si h es una aplicación inyectiva del conjunto K en K'.

DEFINICIÓN. Se denomina *endomorfismo del anillo $\mathcal{K}$* al homomorfismo del anillo $\mathcal{K}$ en el mismo. Un isomorfismo del anillo $\mathcal{K}$ en si mismo es nombrado *automorfismo del anillo $\mathcal{K}$*.

Así como, por ejemplo, se considera como automorfismo a la aplicación idéntica del anillo sobre el mismo.

TEOREMA. 4.2. *Si una aplicación h del anillo $\mathcal{K}$ en el anillo $\mathcal{K}'$hace pasar a la unidad del anillo $\mathcal{K}$ en la unidad del anillo $\mathcal{K}'$, y respeta las operaciones de adicion y de multiplicación, es decir que*

$h\,(x + y) = h\,(x) + h\,(y)$ para todos x, y de K,

$h\,(xy) = h\,(x)\circ h\,(y)$ para todos x, y de K,

además h hace pasar el cero del anillo $\mathcal{K}$ en el cero del anillo $\mathcal{K}'$ y es un homomorfismo.

Demostración. Consideremos los grupos aditivos

$< K,\ +, ->$ y $< K',\ +,\ ->$

Del anillo $\mathcal{K}$ y $\mathcal{K}'$. Por hipótesis, h respeta a la operación de adicion. De donde, en virtud del TEOREMA 3.1, se deduce que h hace pasar el cero del anillo $\mathcal{K}$ en el cero del anillo $\mathcal{K}'$ y es un homomorfismo del grupo $< K,\ +,\ ->$ en el grupo $< K',\ +,\ ->$. En particular, $h\,(-x) = -h\,(x)$ para todo x de K. Por consiguiente, la aplicación h respeta todas las operaciones principales del anillo $\mathcal{K}$ y es un homomorfismo. ■

TEOREMA 4.3. *Una relación de isomorfismo sobre un conjunto cualquiera de anillo es reflexiva, transitiva y simétrica y, por consiguiente, es una relación de equivalencia.*

Este TEOREMA se realiza directamente del TEOREMA 2.5.

Ejemplos. 1. Consideremos el conjunto Q de los números racionales, $Q\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \,\middle|\, a, b \in Q\right\}$. EL álgebra $Q\left[\sqrt{2}\right] = \langle Q\left[\sqrt{2}\right], +, -, \cdot, 1\rangle$ es un anillo. La aplicación $f: Q\left[\sqrt{2}\right] \to Q\left|\sqrt{2}\right|$ definido por la formula $f\left(a + b\sqrt{2}\right) = a -$

$b\sqrt{2}$ es una aplicación inyectiva del conjuto $Q[\sqrt{2}]$ sobre el mismo. La aplicación f respecto a las operaciones principales del anillo $Q[\sqrt{2}]$. De hecho, para todos $x = a + b\sqrt{2}$ y $y = c + d\sqrt{2}$

$f(xy) = f(ac + 2bd + (ad + bc)\sqrt{2} = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = f(x)f(y)$;

$f(x + y) = f(a + b\sqrt{2} + c + d\sqrt{2}) = a - b\sqrt{2} + b - d\sqrt{2} = f(x) + f(y)$;

$f(1_Q) = 1 = 1_{Q[\sqrt{2}]}$.

Por consiguiente, la aplicación f es un automorfismo del anillo $Q[\sqrt{2}]$.

2. Sean K un conjunto de todas las matrices de la forma $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ de a y b racionales y $\mathcal{K} = < K, +, -, \cdot, 1 >$, anillo de tales matrices. La aplicación h: $Q\sqrt{2} \to K$ definido por la formula

$$h(a + b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$$

que constituye una aplicación inyectiva del conjunto $Q\sqrt{2}$ sobre K. Se verifica sin pena que la aplicación h respeta las operaciones principales del anillo $Q[\sqrt{2}]$. h es por lo tanto un isomorfismo del anillo $Q[\sqrt{2}]$ sobre el anillo $\mathcal{K}$.

3. Sea L el conjunto de todas las matrices de la forma $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ llamados *diagonales* con a y b racionales. El álgebra $\mathcal{L} = < L, +, -, \cdot, I >$, donde $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ es un anillo. La aplicación $f: L \to Q$ definida por la formula

$f\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a$ para todos a, b de Q

Es una aplicación que representa las operaciones principales del anillo $\mathcal{L}$. Por consiguiente, f es un homomorfismo del anillo $\mathcal{L}$ sobre el anillo Q de los números racionales.

Sub-anillos. Sea $\mathcal{K} = <$ K, $+, -, \cdot, 1 >$ un anillo.

DEFINICIÓN. Se denomina *sub-anillo del anillo* $\mathcal{K}$ toda sub-álgebra de este anillo.

De acuerdo con la definición de la sub-álgebra se puede definir un sub-anillo con mayores detalles de la siguiente manera. El álgebra $\mathcal{L} = < L, \oplus, \ominus, \odot, 1_{\mathcal{L}} >$ del tipo $(2, 1, 2, 0)$ se denomina *sub-anillo del anillo* $\mathcal{K}$ si $L \subset K$ y si la aplicación idéntica del conjunto L en K es un momorfismo del álgebra $\mathcal{L}$ en $\mathcal{K}$, es decir si se cumplen las condiciones:

(1) $a \oplus b = a + b$ para todos a, b de L;
(2) $\ominus a = -a$ para todo a de L;
(3) $a \odot b = a \cdot b$ para todos a, b de L;
(4) $1_{\mathcal{L}} = 1_{\mathcal{K}}$.

La notación $\mathcal{L} \subset \mathcal{K}$ significa que el álgebra $\mathcal{L}$ es un sub-anillo del anillo $\mathcal{K}$.

Si $\mathcal{L} \subset \mathcal{K}$ se deduce de la definición del sub-anillo que el conjunto L es cerrado respecto a cada operación principal del anillo $\mathcal{K}$ de los elementos de L resultado de nuevo a los elementos del conjunto L. Por otro lado, en virtud de las condiciones $(1) - (4)$ cada operación principal del álgebra $\mathcal{L}$ es una restricción de la operación principal apropiada del anillo $\mathcal{K}$ por el conjunto L.

TEOREMA. 4.4. *Todo subanillo de un anillo es un anillo. El cero y la unidad del anillo que constituyen el cero y la unidad de todos son subanillos.*

Demostración. Sean $\mathcal{L} = < L, \oplus, \ominus, \odot, 1_{\mathcal{L}} >$ un sub-anillo del anillo $\mathcal{K} = <$ K, $+, -, \cdot, 1 >$ y 0 el cero del anillo $\mathcal{K}$. En virtud de las condiciones (1) y (2) el álgebra $< L, \oplus, \ominus >$ es un sub-grupo del grupo aditivo $< K, +, - >$ del anillo $\mathcal{K}$. Del cual el álgebra $< L, \oplus, \ominus >$ es un grupo abeliano y 0 su elemento cero.

En $\mathcal{L}$ la multiplicación es asociativa. De hecho, en virtud de (3), se viene

$a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c$

Para todos a, b, c de L. En virtud de (3) y (4) $1_{\mathcal{L}} = 1$ y $a \odot 1_{\mathcal{L}} = a \odot 1 = a \cdot 1 = a$ para todo a d L. Por consiguiente, el álgebra $< L, \odot, 1_{\mathcal{L}}$ es un monoide.

En $\mathcal{L}$ la multiplicación es distributiva respecto a la adicion. De hecho en virtud de (1) y (3), para todos a, b, c de L

(a $\oplus b) \odot c = (a + b) \cdot c = a \odot b \oplus b \odot c$

Y de manera análoga, se tiene que $c \odot (a \oplus b) = \cdot c \odot a \oplus c \odot b$. Por lo tanto, el álgebra $\mathcal{L}$ es un anillo. ■

Consideremos un anillo $\mathcal{K} = < K, +, -, \cdot, 1 >$ y A un subconjunto cualquiera no vacio del conjunto K cerrado en las operaciones principales del anillo $\mathcal{K}$. Sean $\oplus$, $\ominus$, $\odot$ una restricción de las operaciones principales del anillo $\mathcal{K}$ en el conjunto A, es decir

$a \oplus b = a + b$ para todos a, b de A;

$\ominus a = -a$ para todo a de A;

$a \odot b = ab$ para todos a, b de A.

Mientras que, seguido los TEOREMAs 2.6 y 4.4 el álgebra $\mathcal{A}$

(5) $\mathcal{A} = < A, \oplus, \ominus, \odot, 1 >$,

es un sub-anillo del anillo $\mathcal{K}$. ASi el sub-anillo $\mathcal{A}$ del anillo $\mathcal{K}$ se define de manera unequivoca por un subconjunto no vacio A del conjunto K cerrado en $\mathcal{K}$. Tambien en lugar de (5) se escribe: << el sub-anillo $\mathcal{A} = < A, +, -, \cdot, 1 >$ >> y se lee << el conjunto A es un sub-anillo del anillo $\mathcal{K}$ respecto a las operaciones $+, -, \cdot, 1$ >>.

TEOREMA 4.5. *La relación binaria ~~7~~<< constituir un sub-anillo >>) sobre un conjunto de subanillos del anillo dado es reflexivo, transitivo y anti simétrico, es decir es una relación de orden no estricto.*

Este TEOREMA es un caso especial del TEOREMA 2.8.

TEOREMA 4.6. La intersección de una colección cualquiera (no vacia) de sub-anillos del anillo $\mathcal{K}$ es un sub-anillo del anillo $\mathcal{K}$.

Este TEOREMA es un caso especial del TEOREMA 2.10.

Se deduce del TEOREMA 4.4 que para todo conjunto M de elementos del anillo $\mathcal{K}$ hay un sub-anillo $\mathcal{L}$ minimal que incluye al conjunto M. Se ve sin pena que $\mathcal{L}$ es una intersección de todos los sub-anillos del anillo $\mathcal{K}$ que comprenden el conjunto M. Este sub-anillo minimal $\mathcal{L}$ es nombrado *sub-anillo engendrado por el conjunto* M, M siendo el *sistema de generatrices* para el anillo $\mathcal{L}$.

Ejemplos. 1. Sea D el conjunto de todas las matrices 2×2 diagonales de la forma $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ asociadas al anillo $\mathcal{K}$. El conjunto D es cerrado en las operaciones principales del anillo de todas las matrices 2×2 asociadas al anillo $K, \mathcal{K}^{2\times 2} = < K^{2\times 2}, +, -, \cdot, I >$. El álgebra $< D, +, -, \cdot, 1 >$ es por lo tanto un sub-anillo del anillo $\mathcal{K}^{2\times 2}$.

2. Las matrices de la forma $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ son nombradas *matrices triangulares superiores*. Sea L el conjunto de todas las matrices triangulares superiores asociadas al anillo $\mathcal{K} = < K, +, -, \cdot, 1 >$. El conjunto L es cerrado en las operaciones principales del anillo $\mathcal{K}^{2\times 2} = < K^{2\times 2}, +, -, \cdot, I >$ de las matrices 2×2 sobre $\mathcal{K}$. Por consiguiente, el álgebra $< L, +, -, \cdot, I >$ es un sub-anillo del anillo $\mathcal{K}^{2\times 2}$.

3. Sean $\mathcal{K}$ un anillo cualquiera no nulo y S el conjunto de todas las matrices de la forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ de elementos a, b, de K. Verificando directamente se ve que el conjunto S es formado de las operaciones principales del anillo $\mathcal{K}^{2\times 2} = < K^{2\times 2}, +, -, \cdot, I >$. El álgebra $< S, +, -, \cdot, I >$ es por lo tanto un sub-anillo del anillo $\mathcal{K}^{2\times 2}$.

4. Sea $\mathcal{K} = < K, +, -, \cdot, 1 >$ un anillo de todas las funciones reales definidas y continuas sobre el conjunto R de los números reales. Sea D el conjunto de todas las funciones reales definidas y derivadas sobre el conjunto R. El conjunto D es cerrado en las operaciones principales del anillo $\mathcal{K}$. Por lo tanto, el álgebra $< D, +, -, \cdot, 1 >$ es un sub-anillo del anillo $\mathcal{K}$.

Ejercicios

1. Aclarar si los conjuntos siguientes de los números racionales son cerrados relativamente de las operaciones principales del anillo de los números racionales;
   (a) El conjunto de todos los enteros pares;
   (b) El conjunto de todos los números naturales;
   (c) El conjunto de todos los números racionales cuyos denominadores son la unidad o los números pares:
   (d) El conjunto de todos los números racionales de los denominadores impares.
2. Aclarar si los conjuntos siguientes de números reales son cerrados relativamente de las operaciones principales del anillo de todos los números reales:
   (a) El conjunto de todos los números de forma $a + b\sqrt{2}$ de a y b enteros;
   (b) El conjunto de todos los números de forma $a + b\sqrt{3}$ de a y b enteros;
   (c) El conjunto de todos los números de forma $a + b\sqrt{5}$ de a y b racionales.
3. Considerar un anillo no nulo $\mathcal{K}$. Demostrar que el anillo de las matrices 2×2 sobre $\mathcal{K}$ es un anillo no conmutativo con divisores de cero.
4. Demostrar que en el anillo compuesto de n elementos para cada elemento a del anillo $na = 0$.
5. Demostrar que si el elemento a del anillo es permutable con el elemento b, es decir que $ab = ba$, es igualmente permutable con los elementos $(-b)$, b^{-1} y nb, donde n es un entero: si el elemento a es permutable con los b y c es igualmente permutable con los elementos $b + c$ y bc.
6. Sea $a^2 = a$ para cada elemento a del anillo $\mathcal{K}$. Mostrar que el anillo $\mathcal{K}$ es comutativo.
7. Sea f un homomorfismo del anillo $\mathcal{K}$ en el anillo $\mathcal{K}' =< \mathcal{K}', +, -, \cdot, 1 >$. Mostrar que el álgebra $< Im\, f, +, -, \cdot, 1 >$ es un subanillo del anillo $\mathcal{K}'$.
8. Demostrar que para todos elementos x, y de un anillo conmutativo y de enteros positivos cualesquiera m y n
   (a) $x^m \cdot x^n = x^{m+n}$;
   (b) $(x^m)^n = x^{mn}$;
   (c) $(xy)^n = x^n y^n$.
9. Demostrar que el álgebra isomorfa del anillo es ella misma un anillo.
10. Demostrar para un anillo cualquiera recurriendo a la recurrencia por n el TEOREMA binomial
    $(a + b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \cdots + b^n$,
    Donde n es un entero positivo y $C_n^k = \frac{n!}{k!(n-k)!}$.

§ 5. Sistemas algebraicos.

Noción de sistema algebraico. Sea A un conjunto no vacio cualquiera.

DEFINICIÓN. Se denomina *sistema algebraico* a un triplete ordenado $\mathcal{A} =< A, \Omega, \Omega_0 >$,

Donde A es un conjunto no vacio, Ω el conjunto de operaciones sobre A y Ω_0 el conjunto de relaciones sobre A.

Un sistema algebraico $\mathcal{A}$ es por lo tanto definido por tres conjuntos:

(a) Un conjunto no vacío A notado igualmente $|\mathcal{A}|$; este conjunto es nombrado *conjunto de base del sistema $\mathcal{A}$ y* sus elementos *del sistema $\mathcal{A}$*;
(b) Un conjunto de operaciones Ω definidas sobre A y llamadas *operaciones principales del sistema $\mathcal{A}$*;
(c) Un conjunto de relaciones Ω_0 dadas sobre A y nombradas *relaciones principales del sistema $\mathcal{A}$*;

Si $\mathcal{A} =< A, \Omega, \Omega_0 >$ es un sistema algebraico se dice también que el conjunto A es un sistema algebraico respecto a las operaciones Ω y a las relaciones Ω_0.

Se comprende a veces por sistema algebraico a la pareja $< A, \Omega^* >$, donde $\Omega^* = \Omega \cup \Omega^*$, Ω siendo el conjunto de las operaciones sobre A, y Ω_0 el conjunto de las relaciones sobre A. En este caso si $\Omega_0 = \varnothing$, el sistema $< A, \Omega^* > = < A, \Omega >$ es entonces una álgebra. Se puede por lo tanto así como considerar el álgebra como un caso especial del sistema algebraico.

DEFINICIÓN. Los sistemas algebraicos $\mathcal{A} = < A, \Omega, \Omega_0 >$ y $\mathcal{B} = < B, \Omega', \Omega'_0 >$ son dichos del mismo tipo si las álgebras $< A,\ \Omega >$ y $< B,\ \Omega' >$ son del mismo tipo y que existe una aplicación inyectiva del conjunto Ω_0 sobre Ω'_0 para la cual toda relación $R_{\mathcal{A}}$ de Ω_0 asi como la relación $R_{\mathcal{B}}$ de Ω'_0 que le corresponde en la aplicación son del mismo rango.

El caso encontrado más a menudo es el de los conjuntos Ω y Ω_0 fititos: $\Omega = \{f_1, \dots, f_s\},\ \{R_1, \dots, R_t\}$. En lugar de la notación

$\mathcal{A} = <$ A, $\{f_1, \dots, f_s\},\ \{R_1, \dots, R_t\} >$

Se utiliza generalmente la notación

$\mathcal{A} = <$ A, $f_1, \dots, f_s, R_1, \dots, R_t >$.

En otra se deduce $(r\ (f_1), \dots, r\ (f_s);\ r\ (R_1), \dots, r\ (R_t))$, donde $r\ (f_i)$ es el rango de la operación f_i y $r\ (R_h)$ el rango de la relación R_h, es nombrada *tipo del sistema* $\mathcal{A}$. Los sistemas algebraicos $\mathcal{A}$ y $\mathcal{B}$,

$\mathcal{B} = < B, f'_1, \dots, f'_s, R'_1, \dots, R'_t >$,

son del mismo tipo si sus tipos coinciden, es decir si $r\ (f_i) = r\ (f'_i)$ para $i = 1, \dots, s,\ r\ (R_*) = r\ (R'_k)$ para $k = 1, \dots, t$. Además, la operación f_i del sistema $\mathcal{B}$ es dicho *operación asociada a la operación* f_i del sistema $\mathcal{B}$ es nombrado *relación asociada* a la relación R_k del sistema $\mathcal{A}$.

Ejemplo. Un conjunto de números naturales N con unas operaciones ordinarias de adicion$+$, de multiplicación $\cdot$ y la relación de orden $\leq$ es un sistema algebraico$< N,\ +,\ -,\ \leq >$ del tipo $(2{,}2;\ 2)$.

Isomorfismos de los sistemas algebraicos. Sean $\mathcal{A}$ y $\mathcal{B}$ unos sistemas algebraicos del mismo tipo, $R_{\mathcal{A}}$ una relación principal arbitraria del sistema $\mathcal{A}$ y $\mathcal{B}$ de los sistemas algebraicos del mismo tipo, $R_{\mathcal{A}}$ una aplicación principal arbitraria del sistema $\mathcal{A}$ y $R_{\mathcal{B}}$ la relación principal apropiada del sistema$\mathcal{B}$. Se dice que la aplicación h del conjunto $|\mathcal{A}|$ en $|\mathcal{B}|$ Respecto a la relación $R_{\mathcal{A}}$ si

$(a_{1,\dots}, a_n) R_{\mathcal{A}} \leftrightarrow (h(a_1), \dots, h(a_n)) \in R_{\mathrm{B}}$

Para todos $a_{1,\ \dots,\ a_{1,\ \dots,\ a_n}}$ de $|\mathcal{A}|$,

Donde $''$ es el rango de la relación $R_{\mathcal{A}}$.

Definición. llámese *isomorfismo del sistema algebraico* $\mathcal{A}$ sobre un sistema del mismo tipo $\mathfrak{B}$ la función inyectiva del conjunto $|\mathcal{A}|$ sobre $|\mathfrak{B}|$ respetando a todas las operaciones y relaciones principales del sistema $\mathcal{A}$. Los sistemas $\mathcal{A}$ y $\mathfrak{B}$ son llamados isomorfas si hay isomorfismo del sistema $\mathcal{A}$ sobre $\mathfrak{B}$.

La notación $\mathcal{A} \cong \mathfrak{B}$quiere decir que los sistemas $\mathcal{A}$ sobre $\mathfrak{B}$ son isomorfas.

Definición. llámese *monomorfismo* o *inyección* del sistema algebraico$\mathcal{A}$ sobre el sistema $\mathfrak{B}$ del mismo tipo de aplicación inyectiva del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$ que respeta todas las operaciones y relaciones del sistema $\mathcal{A}$.

Definición. llámese *homomorfismo* del *sistema algebraico*$\mathcal{A}$ en n sistema $|\mathfrak{B}|$ del mismo tipo de aplicación h del conjunto $|\mathcal{A}|$ en $|\mathfrak{B}|$ que respeta a todas las operaciones principales del sistema $\mathcal{A}$que satisface la condición.

$(a_{1,\ \dots,\ a_n}) \epsilon R_{\mathcal{A}} \rightarrow (h(a_1),\ \dots, h(a_n)) \epsilon\ R_{\mathfrak{B}}$

Para todos $a_{1,\ \dots,\ a_{1,\ \dots,\ a_n}}$ de $|\mathcal{A}|$,

Donde $R_{\mathcal{A}}$ es una relación principal cualquiera del sistema $\mathcal{A}$, $''$ son rangos mientras que $R_{\mathfrak{B}}$ es la relación principal del sistema $\mathfrak{B}$ asociado a la relación $R_{\mathcal{A}}$.

SUB-SISTEMAS. sea$\mathcal{A}$ o $\mathfrak{B}$ sistemas algebraicos del mismo tipo, $f_{\mathcal{A}}$la operación principal del sistema $\mathcal{A}$ y $f_{\mathfrak{B}}$ la operación principal o apropiada del sistema $\mathfrak{B}$, $R_{\mathcal{A}}$ la relación principal del sistema $\mathcal{A}$ y $R_{\mathfrak{B}}$ la relaciónprincipal apropiada del sistema $\mathfrak{B}$.

DEFINICIÓN. el sistema$\mathcal{A}$ es llamados sub-sistemas del sistema $\mathfrak{B}$ si $|\mathcal{A}| \subset |\mathfrak{B}|$ asi como para cada operación principal $f_{\mathcal{A}}$ y cada relación principal $R_{\mathcal{A}}$ son completadas con las siguientes condiciones

$f_{\mathcal{A}}\ (a_{1,\ \dots,\ a_m}) = f_{\mathfrak{B}}\ (a_{1,\ \dots,\ a_m})$

Para todos $a_1, \ldots, a_m$ de $|\mathcal{A}|$,

$$(a_1, \ldots, a_n) \in R_{\mathcal{A}} \leftrightarrow (a_n, \ldots, a_n) \in R_{\mathfrak{B}}$$

Para todos $a_1, \ldots, a_n$ de $|\mathcal{A}|$,

Donde $m$es el rango de la operación $f_{\mathcal{A}}$ y n el rango de la operación $R_{\mathcal{A}}$.

Dicho de otra manera el sistema $\mathcal{A}$ es llamado sub-sistema del sistema $\mathfrak{B}$si $|\mathcal{A}| \subset |\mathfrak{B}|$y la función idéntica de $|\mathcal{A}|$ en $|\mathfrak{B}|$ es un monomorfismo del sistema $\mathcal{A}$ en el sistema $\mathfrak{B}$ la notación $\mathcal{A} \rightarrowtail \mathfrak{B}$ quiere decir que el sistema $\mathcal{A}$ es un sub-sistema del sistema B.

Se demuestra de la definición si $\mathcal{A} \rightarrowtail \mathfrak{B}$, el conjunto $|\mathcal{A}|$ está cerrado en el sistema $\mathfrak{B}$ y por consiguiente la operación de toda la operación principal $f_{\mathfrak{B}}$ a los elementos del conjunto $|\mathcal{A}|$ termina de nuevo en los elementos del conjunto $|\mathcal{A}|$.

En virtud (1) cada operación principal $f_{\mathcal{A}}$ del álgebra $\mathcal{A}$ es una restricción de la operación apropiada $f_{\mathfrak{B}}$ para el conjunto $|\mathcal{A}|$, es decir que se tiene $f_{\mathcal{A}} = f_{\mathfrak{B}} | \mathcal{A}|$.

Sea R una relación de rango n sobre el conjunto B y $A \subset B$.

DEFINICIÓN. La relación S de rango n sobre el conjunto Aes llamado *restricción de la relación* Rpor el conjunto Asi $S = R \cap A^n$ lo que equivale a la condición

$$(a_1, \ldots, a_n) \in S \leftrightarrow (a_1, \ldots, a_n) \in R$$

Para todos$a_1, \ldots, a_n$ de$A$.

A partir de esta definición, en virtud de(2)que cada relación principal de un sub-álgebra es una restricción de su relación apropiado por el mismo álgebra.

Sea $\mathfrak{B} = \langle B, f_1, \ldots, f_s, R_1, \ldots, R_t \rangle$es un sistema algebraico y C un sub-sistema cualquiera no vacío del conjunto $|\mathfrak{B}|$ cerrado relativamente a las operaciones principales del sistema $\mathfrak{B}$.señalamos$f_i | C$ y $R_R | C$ las restricciones para el conjunto C de la operación f_i y de3 la relación R_R respectivamente $(i = 1, \ldots, s; k = 1, \ldots, t)$. El sistema

(3) $\mathfrak{C} = \langle C, f_1 | C, \ldots, f_s | C, \ldots, R_t | C \rangle$

es un sub-sistema del sistema $\mathfrak{B}$. Así que el sub-sistema $\mathfrak{C}$del sistema $\mathfrak{B}$ es definido de manera univoca por el subconjunto no vacío C cerrado en el sistema $\mathfrak{B}$ por consecuencia de (3) escribimos « el sub-sistema $\mathfrak{C} = \langle C, f_1, \ldots, f_s; R_1, \ldots, R_t \rangle$ » o bien « el conjunto C es un subsistema relativo a las operaciones $f_1, \ldots, f_s$ o bien a la relación $R_1, \ldots, R_t$ ».

Ejercicios

1. Sea h un isomorfismo del sistema algebraico$\langle A, R \rangle$ sobre el sistema algebraico$\langle B, S \rangle$ o bien R o S son relaciones binarias demostrar que se tiene entonces::
   (a) Si R es reflexivo (sobre A), S también es reflexivo (sobre B) ;
   (b) Si R no es reflexivo (sobre A) , S tampoco es reflexivo (sobre B) ;
   (c) Si la relación R es simétrica, S también lo es ;
   (d) **Si** R es transitiva , S tambien lo es ;
   (e) **Si** R es anti simétrica, S también lo es;
   (f) **Si** R está ligada, Stambién lo está ;
   (g) **Si** R es una relación de orden total (no estricto) (sobre A), Stambién es una relación de orden estricto (no estricto) (sobre B) ;
   (h) **Si** R es una relación de orden total (sobre A), S también es una relación de orden total (sobre B).

2. Mostrar sobre el ejemplo de los sistemas $\langle N, \sigma \rangle$ y $\langle N, > \rangle$ donde σ es una relación binaria vacía sobre N aun cuando N, es del conjunto de los números naturales, que cada homomorfismo mutuamente univoco no es un isomorfismo.
3. Dar ejemplos de isomorfismos y homomorfismos de sistemas algebraicos.

CAPITULO IV
PRINCIPALES SISTEMAS NUMÉRICOS

§ 1. Sistemas de números naturales

Alfabeto y palabras. Se denomina *alfabeto* a una colección arbitraria de símbolos llamados *letras*. Se admite también que las letras pueden repetirse un sin número de veces como caracteres de imprenta. La serie de letras del alfabeto puede enunciarse bajo una forma de lista concreta de letras encerradas en llaves. Se admite que en tal lista no puedan haber repeticiones: las dos letras del alfabeto son diferentes. Supóngase que cada alfabeto posee al menos una letra.

Las letras que componen el alfabeto $\mathfrak{U}$ se denominan letras del alfabeto $\mathfrak{U}$. También se denomina que las letras del alfabeto $\mathfrak{U}$ pertenecen a $\mathfrak{U}$.

Cualquier sucesión finita de letra se denomina palabra. En el alfabeto $\mathfrak{U}$ dado se denomina palabra cada letra que pertenece a este alfabeto. Por ejemplo las palabras $a, ba, baab, baaacb$ son palabras del alfabeto $\{a,\ b,\ c\}$. Las palabras $0, 00, 0|, |, 0\ |, ||\ 00$ pueden considerarse como palabras del alfabeto $\{0,\ |\}$ dado que cada sucesión de letras de un alfabeto escrito una a continuación de la otra es una palabra, en cualquier alfabeto se considera que pueden existir largas palabras tanto como se quiera. Es fácil introducir en el estudio una palabra que no contenga ninguna letra; tal palabra es llamada *palabra vacía.*

Dos palabras son llamadas iguales (iguales gráficamente) si su escritura coincide, es decir si están compuestas por las mismas letras que se disponen idénticamente.

Plantéese que los símbolos A y B designan palabras en un alfabeto cualquiera. Se asocia al par A y B la palabra AB la cual se obtiene escribiéndolas seguido de la palabra A (a la derecha) la palabra B. La palabra AB es llamada *composición* (concatenación) o unión de palabras A y B. Por ejemplo si A conforma la palabra bac y B la palabra aba, AB formaran la palabra $bacaba$. La composición de cualquier palabra con una palabra vacía por definición es considerada igual a la palabra A.

Se da cuenta fácilmente que la concatenación (composición) de las palabras es asociativa: por tres palabras cualquieras A, B, C la composición de palabras AB y C es igual a la composición de palabras A y BC.
Por consiguiente las dos composiciones pueden plasmarse de la misma manera: ABC.

La palabra B es llamada inversión (por reflejo) de la palabra A si B está compuesta por las mismas ocurrencias de letras como A, pero escritas en un orden inverso. Por ejemplo la palabra bac es una inversión de la palabra cab y recíprocamente. Una palabra es llamada simétrica si coincide con su inversión por ejemplo la palabra sis, $bab0\,|\,0$ son palabras simétricas.

La palabra A es llamada sub-palabra de la palabra B si existen palabras como C o E (probablemente vacías) tales como $B = CAE$. Si A es una sub-palabra de B se denomina que A aparece en B. Para A y B dado la palabra A puede poseer muchas coyunturas en la palabra B. Está claro que una palabra vacía es una sub-palabra de cualquier palabra.

Palabras de un alfabeto de una sola letra. Considérese un alfabeto $r = \{|\}$ compuesto por una sola letra « | » llamado bastón vertical. Nótese N^* al conjunto de todas las palabras del alfabeto r en una letra. A El conjunto N^* pertenece la palabra vacía representada 0^*, las palabras | , ||, |||, ||||, etc. si n es una palabra del alfabeto r, $n\,|$ es también una palabra de este alfabeto.

Dos elementos m y n de N^* se denominan iguales y se escriben $m = n$ si ellos son iguales como palabras (iguales gráficamente). Si las palabras m y n no son iguales se escriben $m \neq n$.

DEFINICIÓN. Sean m y n palabras cualquieras del alfabeto r . La composición de palabras m y n lleva el nombre de *suma* de m y n y se denota $m \oplus n$. La operación $\oplus$ es llamada operación de adición.

Por ejemplo, la composición de las palabras || y ||| es la palabra ||||.

Así, ||⊕||| =||||,

La composición de una palabra cualquiera n de N^* y de una palabra vacía 0^* es por definición la palabra n por lo tanto $n \oplus 0^* = n, 0^* \oplus n = n$.

Anteriormente se mencionó que la composición de una palabra es asociativa. En particular, para cualquier elemento m y n de N^* se verifica la igualdad $m \oplus (n \oplus |\ ) = (m \oplus n) \oplus |$ ya que $n \oplus | = n|, m \oplus n|$. La asociatividad de la composición de las palabras permite determinar la suma de tres o más términos:

$k \oplus m \oplus n = (k \oplus m) \oplus n, \qquad k \oplus m \oplus n \oplus l =$

$= (k \oplus m \oplus n) \oplus l$, etc.

DEEFINICIÓN. Se denomina producto de dos palabras m o $n (n \neq 0)$ la palabra igual a la suma de n términos en los que cada uno son igual a m. Además decimos que $m \odot 0^* = 0^*$.

El resultado de las palabras $m\ o\ n$ se denota por $m \odot n$. La operación $\odot$ es llamada multiplicación de las palabras. Así se tiene

$m \odot n = \underbrace{m \oplus m \oplus \ldots \oplus m}$

Por ejemplo para cualquier m de N^* se deduce:

$m \odot | = m, m \oplus || = m \oplus m,$

$m \odot ||| = m \oplus m \oplus m$, etc.

Sistemas de números naturales. Véase el enfoque axiomático de la introducción de números naturales.

DEFINICIÓN. Se denomina *sistemas de números naturales* al álgebra $\langle N, +, ., 0, 1\rangle$ compuesto de algún conjunto N, de elemento 0 y 1 separados de N, de operaciones binarias + y · (llamadas adición y multiplicación) que satisface las condiciones siguientes (axiomas)

I. Para cualquier n de $Nn + 1 \neq 0$.

II. Para cualquier m y n de N si $m + 1 = n + 1$, se tiene $m = n$.

III. Para cualquier m de $Nm + 0 = m$.

IV. Para cualquier m y $nm + (n + 1) = (m + n) + 1$.

V. Para cualquier m de $Nm. 0 = 0$.

VI. Para cualquier m y n de $Nm. (n + 1) = m.n + m$.

VII. Si A es un sub-conjunto del conjunto N tal como (a) 0 ∈ A , (b) para cualquier n, si $n \in A$, también se tiene $n + 1 \in A$, es decir $A = N$.

El sistema de axioma antes mencionado se denomina *sistema de axiomas de Peano* dado que es una variante insensible de la axiomática propuesta por el matemático italiano Peano.

La condición I Quiere decir que el elemento 0 no se puede representar bajo forma de suma de un elemento cualquiera de N y del elemento 1. La condición II Quiere decir que el elemento 1 es regular a la izquierda con respecto a la adición. La condición III Indica que 0 es un elemento neutro a la derecha con respecto a la adición. La condición IV traduce la forma débil de la asosiatividad de la adición. La condición VI es una forma débil de la distributividad de la multiplicación con respecto a la adición. La condición VII *es llamada axioma de la inducción matemática*. A partir de este axioma se deduce el hecho que cualquier subconjunto del conjunto N que contenga $0,1$ cerrado con respecto a la adición y coincide con el conjunto N. Así que el axioma inducción matemática se deriva que el único sub-álgebra del álgebra $\mathcal{N} = \langle N, |, .,\ 0,1\rangle$es el mismo álgebra $\mathcal{N}$.

Los elementos del conjunto $\mathcal{N}$ son llamados números naturales. Los elementos 0 y 1 son llamados respectivamente *cero* y *unidad del sistema* $\mathcal{N}$.

Para las notaciones de números $1+1, (1+1)+1, \big((1+1)+1\big)+1, \Big(\big((1+1)+1\big)+1\Big)+1, \ldots$ se utiliza la simbología decimal banal $2, 3, 4, 5, \ldots$

Se pregunta: ¿existe al menos un sistema de números naturales, es decir un álgebra de tipo $(2, 2, 0, 0)$ que satisface a los axiomas I-VII? el ejemplo siguiente proporciona una respuesta afirmativa a la pregunta planteada.

Considérese el conjunto N^* de un alfabeto r a una letra. Se definieron las operaciones $\oplus$ y $\odot$ sobre las palabras del alfabeto r. Supóngase que la palabra vacía 0^* y la palabra $\big|$ juegan respectivamente el papel de cero y de la unidad en el álgebra:

$\mathcal{N}^* = \langle \mathcal{N}^*, \oplus, \odot, 0^*, \big| \rangle$.

Esta álgebra satisface al sistema de axioma I-VII de hecho Para cualquier n de N^* la palabra $n\big|$ no es vacía; así que $n \oplus \big| \neq 0^*$ por lo tanto se satisface la condición I. Ya que para cualquier $m, n \in N^*$ de la igualdad grafica de las palabras $m \big| n$ se deduce la igualad grafica de las palabras m y n, se cumple la condición II. La composición de cualquier palabra m de N^* y de palabra vacía 0^* es la palabra $m, m \oplus 0^* = m,$ es decir que se cumple la condición III. De la asociatividad de la composición de las palabras se deduce que la condición IV está completa. La satisfacción de la condición V se deduce directamente de la definición de la operación de la multiplicación de las palabras. De la igualdad grafica de las palabras

$\underbrace{mm \ldots m}_{n+1\ vez}$ y $\underbrace{mm \ldots m}_{n\ vez}$

Se deduce la igualdad $m \odot \big(n \oplus \big|\big) = (m \odot n) \oplus m$, en la que la condición VI está igualmente completa. En fin es intuitivamente evidente que para el álgebra $\mathcal{N}^*$ el axioma de inducción está satisfecha: si el conjunto $A \subset N^*$ es tal como$(a) 0^* \in A\ y\ (b)$ para cada n si $n \in A, n\big| \in A$ y por consiguiente, $A = \mathrm{N}^*$. De hecho se designa para $A(n)$ el predicado « $n \in A$ » se escribe para cualquier n la secuencia de las implicaciones verdaderas conforme a (b):

$A(0^*) \to A\big(\big|\big), A\big(\big|\big) \to A\big(\big|\big|\big), \ldots, A(n) \to A\big(n\big|\big)$.

Ya que $A(0^*)$ es verdadero se deduce de la primera implicación de la autenticidad de $A\big(\big|\big)$; de la autenticidad de $A\big(\big|\big)$ y de la segunda implicación se deriva la autenticidad de $A(|\,|)$, etc. Después $n+1$ etapas se llega a la conclusión que $A\big(n\big|\big)$ es para cualquier n de $\mathcal{N}^*$.

Principio de la inducción matemática (o de recurrencia). El axioma de la inducción matemática es la base del método de demostración por recurrencia. La demostración por recurrencia es aplicable cuando se trata de demostrar que un predicado singular (en un lugar) en una variable natural libre (condición singular) es verdadero para todos los números naturales.

TEOREMA 1.1 sea $A(n)$ *un predicado singular cualquiera sobre el conjunto* N *de los números naturales que satisface las condiciones:* $(\propto)\ A(0)$ *es verdadero* $\big(0\ satisface\ al\ predicado\ A(n)\big); \beta$ *para cada* n *de* N*, si* $A(n)$*es verdadero,* $A(n+1)$ *también lo es. Entonces* $A(n)$ *es verdadero para cualquier* n *natural.*

Demostración. Sea $A = \{n \in N\ |A(n)\}$. Conforme a $(\propto)$ y β se verifican las siguientes condiciones: $(a) 0 \in A, (b)$ para cualquier $n\ de\ N$ si $n \in A$, también se tiene $n+1 \in A$. Según el axioma VII se deduce que $A = N$. Esta última igualdad quiere decir que cualquier número natural n satisface a la condición $A(n)$. □

El TEOREMA 1.1 no es más que otro enunciado del axioma de inducción matemática y se denominará *principio de la recurrencia matemática*. El principio de la recurrencia matemática que puede plasmarse bajo la forma

$$A(0) \bigwedge \forall n \big(A(n) \to A(n+1)\big) \to \forall n A(n)$$

O bien bajo la forma

$$\frac{A\,(0) \wedge \forall n\ \big(A\,(n) \to A\,(n\ +1)\big) \to \forall n A\,(n)}{\forall n A\,(n)}$$

Principales fases de la Demostración por rrecurencia: 1) se demuestra que 0 satisface a la condicion A ; 2) se demuestra que para cualquier n de $\mathrm{A}(n)$ Se deduce $\mathrm{A}(n\ +1)$. La variable n es llamada *variable sobre la cual se efectúa la recurrencia.* La parte de la demostración que se lee: «es verdadero que $A\ (0)$» es denominado principio de la recurrencia o base de la recurrencia. La segunda parte de la demostración que se lee: «para cualquier n de $\mathrm{A}(n)$» se denomina *hipótesis de recurrencia.*

Para demostrar esta afirmación

$\forall n\ \big(A\,(n) \to A\,(n\ +1)\big)$

Se toma un entero natural cualquiera denotándolo por una letra arbitraria, por ejemplo k, y se demuestra la aplicación $A\,(k) \to A\,(k\ +1)$ que sigue la vía habitual: se supone que $A\,(k)$ es verdadera (hipótesis de recurrencia) y se muestra que entonces $A\,(k\ +1)$ es verdadera.

Ejercicios:

1. Demostrar por recurrencia sobre n que $1 + 2 + \ldots + n = n(n+1)\ /\ 2$.
2. Demostrar por recurrencia sobre n que el conjunto de n elementos posee 2^n sub-conjuntos.
3. Sean $\mathcal{A}$ y B conjuntos finitos compuestos de m y de n elementos respectivamente. Demostrar por recurrencia sobre n que:

(a) El número de aplicación por recurrencia del con conjunto A en B es igual a $n(n-1).\ \ldots(n-m\ +1)$;

(b) El número de todas las aplicaciones posibles del conjunto A en B es igual a n^m.

4. Demostrar que si A es un sub-conjunto del conjunto de números naturales y que por alguna n_0 de A satisface la condición: si para cada número natural n para $n \geq n_0$ de $n \in A$ se deduce que $n\ +1 \in A$, entonces cada número natural $n \geq n_0$ pertenecen al conjunto A.
5. Demostrar por recurrencia sobre n que la composición de funciones inyectivas $f_n \circ f_{n-1} \circ \ldots \circ f_1$ es una función inyectiva.
6. Demostrar la afirmación siguiente (principio de Dirichlet): si es necesario repartir más de n objetos entre n lugares al menos uno de esos últimos contendrá más de un objeto.
7. Escribir los axiomas I-VII del sistema de los números naturales ajustándose al lenguaje de la lógica de los predicados (reemplazando el axioma VII por el principio de recurrencia que le es equivalente)
8. Dar un ejemplo de álgebra del tipo (2, 2, 0, 0) que

(a) Satisface a los axiomas II, VII pero no satisface al a axioma I (del sistema $\mathcal{N}$);

(b) Satisface a los axiomas I, VII y no satisface a el axioma II (del sistema $\mathcal{N}$);

(c) Satisface a los axiomas I, II y no satisface al axioma VII (del sistema $\mathcal{N}$).

§ 2. Propiedades de la adición y de la multiplicación de los números naturales

Propiedades de la adición. La adición de los números naturales verifica las propiedades siguientes (axiomas):

IV. para cada m de $Nm\ + 0 = m$.

V. para cualquier m y n de $Nm\ +\ (n\ +1) =\ (m+n) + 1$.

Estas propiedades permiten para cualquier número natural fijo en m calcular la suma $m + n$ sucesivamente para los valores de n iguales a $0,\ 1,\ 2,\ \ldots$ por lo tanto, estas propiedades permiten obtener la suma de $m + n$ para cualquier número natural m y n.

Sean, por ejemplo, $m = 5$ y $n = 3$. Sirviéndose de las condiciones III, IV y V se está en la medida de escribir la siguiente sucesión de igualdades:

$5 + 0 = 5; 5 + 1 = 6; 5 + 2 = 5 + (1 + 1) = (5 + 1) + 1 = 6 + 1 = 7;$

$5 + 3 = 5 + (2 + 1) = (5 + 2) + 1 = 7 + 1 = 8; asi\ que\ 5 + 3 = 8.$

TEOREMA 2.1 *la adición de números naturales es asociativa es decir que para cualquier* a, b, c *naturales*, se tiene

(1) $a + (b + c) = (a + b) + c$

Demostración. Fíjese de los números naturales cualquier a y b. La fórmula (1) define entonces un predicado en una variable libre c notado A (C). La demostración es conducida por recurrencia sobre la variable natural c.

Base de recurrencia: A (0) es verdadera dado que es verdadera la igualdad

$a + (b + 0) = (a + b) + 0.$

No recurrente. Supóngase que para alguna n natural $A(n)$ es verdadera, es decir que la fórmula es verdadera

$a + (b + n) = (a + b) + n$

Y demuéstrese entonces que es verdadera $A\ (n + 1)$, dicho de otra manera, la fórmula

$a + \big(b + (n + 1)\big) = (a + b) + (n + 1)$

De hecho

$a + \big(b + (n + 1)\big) = a + \big((b + n) + 1\big)$ (Según el axioma IV);

$= \big(a + (b + n)\big) + 1$ (Según el axioma IV);

$= \big((a + b) + n\big) + 1$ (Siguiendo la hipótesis de recurrencia);

$= (a + b) + (n + 1)$ (Según el axioma IV)

Según el principio de recurrencia, el predicado $A(c)$ es verdadero para cualquier c natural. Dado que se fijó la demostración de los valores arbitrarios de a y b, la fórmula (1) se vuelve verdadera para cualquier a y b naturales. □

DEFINICIÓN. El álgebra $\langle N,\ +,\ 0\rangle$ se denomina *monoide aditivo de los números naturales.*

Lema 2.2 para cualquier a y b naturales se tiene

(1) $(a + 1) + b = a + (b + 1).$

Demostración. Hágase la demostración por recurrencia sobre b. Fíjese el número natural arbitrario a. Nótese por $B(b)$ el predicado definido por la fórmula (1). Considérese que en este lema así como más adelante en este caso de análogos $B(b)$ es igual la notación de la fórmula correspondiente.

Vemos sin duda que la fórmula

$B\ (0)\colon (a + 1) + 0 = a + (0 + 1)$

Es verdadera, admítase que para algún número natural n es igualmente verdadera a la fórmula

$B(n)\colon (a + 1) + n = a + (n + 1),$

Y muéstrese que la fórmula $B\ (n + 1)$ es verdadera. En efecto

$(a + 1) + (n + 1) = \big((a + 1) + n\big) + 1$ (Según el axioma IV)

$= \big(a + (n + 1)\big) + 1$ (Al seguir la hipótesis de recurrencia)

$= a + \big((n + 1) + 1\big)$ (Según el axioma IV)

Según el principio de recurrencia, la fórmula $B(b)$ es verdadera para cualquier número natural b dado que la demostración fijó el valor arbitrario de a, la fórmula (1) es verdadero cualesquiera que sean a y b naturales. □

TEOREMA 2.3 *la adición de los números naturales es conmutativa es decir que para cualquier* a, b *naturales, se tiene*

$(1)\ \ a + b = b + a.$

Demostración. Esta se efectúa por recurrencia sobre b.

Demuéstrese primero que la fórmula

$A\ (0)$: $a + 0 = 0 + a$

Es verdadero. Analícese por recurrencia sobre a. La fórmula es aparentemente verdadero para $a = 0$. Después, si por un cierto de numero natural n

$n + o = 0 + n$,

Entonces se deduce

$(n + 1) + 0 = n + (0 + 1)$ (Al seguir el lema 2.2);

$= (n + 0) + 1$ (Al seguir el axioma IV);

$= (0 + n) + 1$ (Al seguir la hipótesis de recurrencia);

$= 0 + n(n + 1)$ (Al seguir el axioma IV).

Por lo tanto, en virtud del principio de recurrencia la fórmula $A(0)$ es verdadero para cualquier a.

Fíjese la elección de a arbitraria. Nótese $A(b)$ el predicado definido por la fórmula (1). Supóngase que por un cierto número natural n la fórmula

$A\ (n)$: $a + n = n + a$

Es verdadero entonces

$a + (n + 1) = (a + n) + 1$ (Según el axioma IV)

$= (n + a) + 1$(Al seguir la hipótesis de recurrencia)

$= n + (a + 1)$(Según el axioma IV)

$= (n + 1) + a$ (Según el lema 2.2)

Es decir que la fórmula $A\ (n + 1)$ es verdadera. Según el principio de recurrencia la fórmula $A\ (b)$ es verdadera para cualquier b. Dado que el valor de a fue fijado de manera cualquiera, la fórmula (1) se vuelve verdadera para cualquier a y b naturales. □

TEOREMA 2.4 (REGLA DE SIMPLIFICACIÓN DE LA ADICIÓN). Para cualquier a, b, c natural, se tiene

(1) Si $a + c = b + c\ entonces\ a = b$.

Demostración (por recurrencia sobre c con elección fijada de los valores arbitrarios a y b) consideramos la fórmula

$A\ (c)$: $(a + c = b + c) \rightarrow\ (a = b)$.

Dado que $a + 0 = a\ y\ b + 0 = b$, es verdadero que

$(a + 0 = b + 0) \rightarrow (a = b)$,

Es decir que la fórmula $A\ (0)$ es verdadera.

Supóngase que para un cierto número natural de n

$A\ (n)$: $\ (a + n = b + n) \rightarrow (a = b)$,

Y demuéstrese que la fórmula $A\ (n + 1)$ es verdadera según el axioma IV

(1) $a + (n + 1) = (a + n) + 1,\ \ b + (n + 1) = (b + n) + 1.$

Luego, según el axioma II

(2) $\big((a + n) + 1 = (b + n) + 1\big) \rightarrow (a + n = b + n).$

$A(n)$ y (3) al ser verdaderos se deduce que

(3) $\big((a + n) + 1 = (b + n) + 1\big) \rightarrow (a = b)$

Es verdadero. Sobre la base de (2) y (4) se concluye que la fórmula

$A(n + 1)$: $\big(a + (n + 1) = b + (n + 1)\big) \rightarrow a = b$

Es verdadera.

Según el principio de recurrencia la fórmula $A(C)$ es verdadera para cualquier c natural. Dado que la elección de a y b era arbitraria la afirmación (1) es verdadera para cualquier a, b, c naturales. □

COROLARIO: 2.5 *para cualquier a y b naturales, si* $b \neq 0$ *se tiene* $a \neq a + b$.

TEOREMA: 2.6 para cualquier número natural a sea $a = 0$, o exista un numero natural b tal como $a = b + 1$

Demostración. Considérese la fórmula

$A\ (a)$: $(a = 0) \vee \exists b(a = b + 1)$.

La demostración de esta fórmula está hecha por recurrencia sobre a. La fórmula es aparentemente verdadera para $a = 0$. Supóngase que para un cierto número natural n la fórmula

$$A\ (n)\text{: } (n = 0) \vee \exists b(n = b + 1)$$

Es verdadera. Es necesario demostrar que la fórmula

$$A\ (n + 1)\text{: } (n + 1 = 0) \vee \exists b(n + 1 = b + 1)$$

Es verdadera. Esta fórmula es efectivamente verdadera, ya que el segundo miembro de la disyunción es una fórmula verdadera $(para\ b = n,\ n + 1 = b + 1)$. Según el principio de recurrencia la fórmula $A\ (a)$ es verdadera para cualquier a natural □

COROLARIO 2.7 *para cualquier a y b naturales, si $a \neq 0$ u $b \neq 0$ se tiene $aa + b \neq 0$.*

Demostración. Plantéese $b \neq 0$, entonces según el TEOREMA 2.6 existe un tal c natural por el cual $b = c + 1$. En virtud del axioma IV

$a + b = a + (c + 1) = (a + c) + 1$.

Según el axioma I $(a + c) + 1 \neq 0$; así que $a + b \neq 0$. □

COROLARIO 2.8 *para cualquier a y b naturales si $a + b = 0$, entonces $a + 0$ y $b + 0$.*

TEOREMA 2.9*. Para cualquier a y b naturales de las tres condiciones solo una es verdadera:*

$(\alpha)a = b$; $(\beta)a + k = b$ (Para un cierto $k \ni N \setminus \{0\}$)

$(\gamma)a = b + m$ (b (Para un cierto $k \ni N \setminus \{0\}$)

Demostración. A partir del corolario 2.5 se deduce que de las tres condiciones solo una puede ser satisfecha. De hecho si las condiciones (α) y (β) fueran completadas, se tendría $a = b + k$ y $k \neq o$, lo que es imposible en virtud del corolario 2.5. Si esas son las condiciones (α) y (γ) que fueron cumplidas, se tendría $b = b + m$ y $m \neq 0$, lo que es imposible. Si esas son las condiciones de (β) y (γ) que fueron satisfechas, se tendría $a = a + k(k + m)$ y $k + m \neq 0$ que sería lo contrario al corolario 2.5.

Demuéstrese ahora que al menos una de las condiciones (α), (β), (γ) se cumplió. Fíjese el numero natural arbitrario a y nótese $A\ (b)$ la disyunción de las condiciones (α), (β) y (γ). Demuéstrese por recurrencia sobre (b) la autenticidad de la fórmula $A\ (b)$la disyunción de las condiciones (α), (β), (γ) y demuéstrese por recurrencia sobre b la autenticidad de la fórmula $A(b)$. La fórmula $A(0)$ es verdadera. De hecho, si $b = 0$, se tiene sea $a = 0$, o $a \neq 0$. Si $a \neq 0, a = 0 + m$, donde $m = a \neq 0$. Así que para $b = 0\ se\ satisface$, ya sea la condición (α), o condición (γ).

Supóngase que para un cierto número n es verificada la fórmula

$A\ (n)$: $(a = n) \vee$ $(a + k = n$ Para un cierto $k \in N \setminus \{0\} \vee$

$$\vee\ (a = n + m\text{Para un cierto } m \in N \setminus \{0\}),$$

Y demuéstrese entonces que la fórmula a $A\ (n + 1)$ es verdadera. En efecto, si $a = n$, entonces $a + 1 = b + 1$ y la condición (β) se cumple. Si $a + k = n$, $a + (k + 1) = n + 1$ y es la condición (β) la que se cumple. Si, por el contrario $a = n + m, a + 1 = (n + 1) + m$ y $m \in$ N $\setminus \{0\}$. En ese caso si $m = 1, a + 1 = (n + 1) + 1$ y según el axioma II $a = n + 1$, la condición (α) se cumple. Dado que $m \neq 0$, según el TEOREMA 2.6 existe una $k \neq 0$ por lo cual $m = k + 1$. Si $m \neq 1$ entonces $k \neq 0$ y de la igualdad $a + 1 = (n + 1) + (k + 1) = \big((n + 1) + k\big) + 1$ según el axioma II se deduce $a = (n + 1) + k, k \neq 0$, la condición (γ)se cumple. En resumen, en todos los casos la fórmula $A\ (n + 1)$ es verdadera. Según el principio de recurrencia la fórmula $A\ (b)$ es verdadera para cualquier b natural. Ya que la elección de a es fijada arbitrariamente la afirmación del TEOREMA para cualquier a y b naturales. □

DEFINICIÓN. Se denomina *diferencia de dos números naturales* a y b un número natural k por el cual $b + k = a$.

Se deduce del TEOREMA 2.9 que la diferencia de dos números naturales a y b existe en caso que la condición (α) sea satisfecha (con $k = 0$) o la condición (γ). O en el caso donde es satisfecha la condición (β) la diferencia de los dos números a y b es inexistente.

Se demuestra sin duda que si la diferencia de los números a y b existe, es única. De hecho, si $b + k = a$ y $b + m = a$ entonces se tiene $b + k = b + m$, donde según la regla de simplificación de la adición se deduce $k = m$.

El numero natural único que constituye la diferencia de los números a y b se señala $a - b$.

Propiedades de la multiplicación. Sea **N** un conjunto de todos los números naturales.

La multiplicación de los números naturales es definida por las condiciones siguientes (axiomas):

V. $m.0 = 0$para cada m deN.

VI. $m(n + 1) = m.n + m$ para cualquier m, n de N.

Se demuestra de esas condiciones que

$m.1 = m$,

$m.2 = m\,(1 + 1) = m + m$,

$m.3 = m(2 + 1) = m.2 + m = (m + m) + m = m + m + m$, etc.

Así que una multiplicación es una adición repetida del número con el mismo.

TEOREMA 2.10. LEY DE LA DISTRIBUTIVIDAD CON EL DERECHO DE LA MULTIPLICACIÓN CON RESPECTO A LA ADICIÓN) *para cualquier $a, b\ y\ c$ naturales se tiene*

(1) $(a + b).c = a.c + b.c$.

Demostración. Fíjese arbitrariamente los valores de $a\ y\ b$. Nótese $A\ (c)$ el predicado definido en ese caso por la fórmula (1). La demostración es guiada por recurrencia sobre la variable natural c. Según el axioma V la fórmula

A: $(0)(a + b).0 = a.0 + b.0$ Es verdadera.

Supóngase que por un número natural cualquiera n la fórmula

$A\ (n)$: $(a + b).n = a.n + b.n$

Es verdadera. Se tiene entonces

$(a + b).(n + 1) = (a + b).n + (a + b)$ (Según el axioma VI);

$= (a.n + b.n) + (a + b)$ (Que sigue la hipótesis de recurrencia)

$= (a.n + a) + (b.n + b)$ (En virtud de la asosiatividad y de la conmutatividad de la adición);

$= a(n + 1) + b(n + 1)$ (Según el axioma VI),

Es decir que la fórmula $A\ (n + 1)$ es verdadera. Según el principio de recurrencia $A\ (c)$ es verdadera para cualquier c natural. Ya que se fijó los valores arbitrarios de a y b, la fórmula (1) sigue siendo verdadera para cualquier a, b y c naturales. □

Lema 2.11 *para cualquier número natural a se tiene* $1.a = a$.

Demostración (se efectúa por recurrencia sobre a). Según el axioma V, se tiene $1.0 = 0$. Supóngase que $1.n = n$ para un número natural cualquiera n. Entonces $1.(n + 1) = 1.n + 1 = n + 1$, es decir $1.(n + 1) = n + 1$. Según el principio de recurrencia la fórmula $1.a = a$ es verdadera para cualquier número natural a.□

TEOREMA 2.12 *la multiplicación de los números naturales es conmutativa, es decir que para cualquier a y b natural, se deduce*

(1) $a.b = b.a$.

Demostración. Recurriendo a la recurrencia sobre a demuéstrese que para cualquier a la fórmula

$A\ (0)$: $a.0 = 0.a$

Es verdadera. Fíjese arbitrariamente el valor de a en la fórmula (1). Nótese $A\ (b)$ el predicado definido por la igualdad (1). Supóngase que para un cierto número natural n se comprueba la fórmula

$A(n)\colon a.n = n.a.$

Entonces se deduce

$a.(n+1) = a.n + a$ (Según el axioma VI);

$= n.a + 1$ (Que sigue la hipótesis de recurrencia);

$= n.a + 1.a$ (Según el lema 2.11);

$= (n+1).a$ (En virtud de la distributividad de la multiplicación con respecto a la adición)

Es decir que se comprueba la fórmula $A\ (n+1)$. Según el principio de recurrencia $A\ (b)$ es verdadera para cualquier b natural. Ya que se fijó el valor arbitrario de a, la fórmula (1) es verdadera para cualquier a y b natural.□

De los TEOREMAs 2.10 y 2.12 se deduce el siguiente TEOREMA

TEOREMA 2.13 (Ley de distributividad a la izquierda de la multiplicación con respecto a la adición). *Para cualquier a, b y c naturales se comprueba la igualdad* $c\ (a+b) = c.a + c.b$.

TEOREMA 2.14 *la multiplicación de los números naturales es asociativa, es decir que para cualquier a, b y c naturales se tiene*

(1) $a(bc) = (ab)c$.

Demostración (Se efectúa por recurrencia sobre *c)* señálese $A\ (c)$el predicado definido por la fórmula (1) con una elección de valores fijadas de a y de b. Según el axioma V, se deduce $b.0 = 0$ y $(a.b).0 = 0$ así que la fórmula

$A\ (0)\colon a\ (b.0) = (a.b).0$

Es verdadera. Suponemos que para un cierto número natural n se comprueba la fórmula

$A(n)\colon a(b.n) = (a.b).n.$

Entonces se deduce

$a.\big(b.(n+1)\big) = a.(b.n+b)$ (Según el axioma VI)

$= a.(b.n) + a.b$ (Según el TEOREMA 2.13);

$= (a.b).n + a.b$ (Que sigue la hipótesis de recurrencia);

$= (a.b).n + (a.b).1$ (Según el axioma V);

$= (a.b)(n+1)$ (Según el TEOREMA 2.13),

Dicho de otra manera, la fórmula $A\ (n+1)$ es verdadera. Según el principio de recurrencia la fórmula $A\ (c)$ es verdadera para cualquier c natural. Ya que fíjese los valores arbitrarios de a, b, la fórmula (1) es verdadera para cualquier número natural a, b y c.□

DEFINICIÓN. El álgebra ⟨N, ., 1⟩ *se denomina monoide multiplicativo de los números naturales.*

TEOREMA 2.15 para cualquier número natural a y b si $a \neq b$ y $b \neq 0$ se tiene $ab \neq 0$.

Demostración. Supóngase que $a \neq b$ y $b \neq 0$. Según el TEOREMA 2.6 existen números naturales m y n para los cuales $a = m+1$ y $b = n+1$. En virtud de los axiomas VI y IV, se tiene

$a.b = a.(n+1) = a.n + a = a.n + (m+1) = (a.n+m) + 1.$

Según el axioma I $(a.n+m)+1 \neq 0$. Así que $a.b \neq 0$.□

TEOREMA 2.16 (REGLA DE SIMPLIFICACIÓN DE LA MULTIPLICACIÓN) para cualquier a, b, c natural si $ac = bc$ y $c \neq 0$, se tiene $a = b$.

Demostración. por hipótesis,

(1) $ac = bc, \quad c \neq 0.$

Plantéese $a \neq b$ según el TEOREMA 2.8 o bien exista una k tal como $a + k = b$ y $k \neq 0$ o bien una m tal como $a = b + m$ y $m \neq 0$. En el primer caso $bc = ac + kc$ y en virtud de (1) $bc = bc + kc$, (lo que según el corolario 2.5) es imposible,

puesto que $k \neq 0$, $c \neq 0$ y (según el TEOREMA 2.15) $kc \neq 0$. En el segundo caso un razonamiento análogo demuestra que con la hipótesis $a \neq b$, el resultado es una contradicción. □

Ejercicios

1. Demostrar las fórmulas:
   (a) $1 + 3 + 5 + \ldots + (2n + 1) = (n + 1)^2$
   (b) $1^2 + 2^2 + \ldots + n^2 = n(n + 1)(2n + 1)/6$;
   (c) $1.2 + 2.3 + \ldots + (n - 1)n = (n - 1)n(n + 1)/3$ para $n > 1$;
   (d) $(1 + 2 + \ldots + n)^2 = 1^3 + 2^3 + \ldots + n^3$;
   (e) $1^2 + 3^2 + \ldots + (2n - 1)^2 = n(2n - 1)(2n + 1)/3$.

2. Demostrar que el numero c_n^k de los subconjuntos que contienen k elementos del conjunto de n elementos $1 \leq k \leq n$ se puede representar por la fórmula
$$c_n^k = \frac{n(n-1)\ldots(n-k+1)}{1.2\ldots k}.$$
3. Demostrar que $c_{n+1}^k = C_n^k + C_n^{k-1}$ para $n \geq k > 1$.
4. Demostrar que para cualquier n natural $(n > 1)$
$$(x + 1)^n = x^n + C^1_{n}x^{n-1} + C^2_{n}x^{n-2} + \ldots + c_n^n$$
5. Demostrar que $1 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$.
6. Demostrar que $\sum_{k=0}^{n}(C_n^k)^2 = C_{2n}^n$.
7. Demostrar que para cualquier número natural a, b, c y d la suma $a + b + c + d$ es independiente del orden de los términos.

§ 3. Relación de orden sobre un conjunto de los números naturales

Relación de orden. Considérese la relación de orden sobre un conjunto de números naturales.

DEFINICIÓN. Si para números naturales a y b existe un número natural k tal como $a + k = b$ y $k \neq 0$, entonces dice que «a es inferior a b» y se le escribe $a < b$. Se dice que « a es inferior o igual a b» y se le escribe $a \leq b$ si $a < b$ o $a = b$.

La relación inversa de la relación < se denota con el símbolo >. Así que, $a > b$ si y solo si $b < a$. Si $a > b$ o $a = b$ se dice que «a es superior o igual a b» y se le escribe $a \geq b$. La relación $\geq$ es la inversa de la relación $\leq$.

TEOREMA 3.1 *Para cualquier número natural* a y b*, se deduce*:

(1) Si $a < b$, entonces $a + 1 \leq b$;
(2) $0 \leq a$;
(3) $a \neq 0$, entonces $0 < a$;
(4) $a \leq b$*si y solo si, existe un numero natural* k *tal como* $a + k = b$

La demostración del TEOREMA se deduce fácilmente de las DEFINICIÓNes de las relaciones < y $\leq$; se deja a criterio del lector la reformulación.

DEFINICIÓN. El sistema algebraico $\langle \mathrm{N}, +, \cdot, < \rangle$ *se denomina sistema ordenado de los números naturales.*

THEOREMA 3.2 (LEY DE LA TRICOTOMIA DE $<$). *Para cualquier número natural* a *y* b *una y solo una de las tres condiciones* $a < b, a = b, a > b$ *se cumple.*

Este TEOREMA se deriva directamente de la definición de la relación $<$ y del TEOREMA 2.9.

COROLARIO 3.3. *Para cualquier número natural* a *y* b *se tiene:*

(1) $a \leq a$ (*reflexibilidad de* $\leq$);
(2) *Sea* $a \leq b$, *sea* $b \leq a$ (*reporte de conexión de* $\leq$);
(3) *Si* $a \leq b$ y $b \leq a$, *entonces* $a = b$ (*anti-simetría de* $\leq$).

TEOREMA 3.4. *La relación binaria $<$ sobre un conjunto de números naturales y transitiva, es decir que para cualquier número natural a, b y c si $a < b$ y $b < c$, se tiene $a < c$.*

Demostración. Supóngase que $a < b$ y $b < c$. Entonces existen números naturales k y m que satisfacen a las condiciones:

(1) $a + k = b, \quad b + m = c;$

(2) $k \neq 0, \qquad m \neq 0.$

En virtud de (1) $a + (k + m) = c$, además, en virtud de (2) y del corolario 2.7, $k + m \neq 0$; así que $a < c$. □

COROLARIO 3.5. *La relación $<$ sobre un conjunto de números naturales es una relación de orden total estricto. El sistema $\langle \mathrm{N}, < \rangle$ es un conjunto totalmente ordenado.*

COROLARIO 3.6. *Para cualquier número natural a, b y c, se tiene:*

(1) Si $a \leq b$ y *$b < c$, entonces $a < c$;*

(2) Si $a < b$ y *$b \leq c$, entonces $a < c$;*

(3) *Si $a \leq b$* y *$b \leq c$, entonces $a \leq c$.*

COROLARIO 3.7. *La relación binaria $\leq$ sobre un conjunto de números naturales es una relación de orden total no estricta.*

TEOREMA 3.8. *La relación $<$es monótona con respecto a la adición y a la multiplicación, es decir que para todos los números naturales a, b y c, se tiene:*

(1) $a < b$ si y solo si $a + c < b + c$;

(2) Si *$a < b$* y *$c \neq 0$, entonces $ac < bc$.*

Demostración. La condición $a + c < b + c$ es equipotente a la condición $a + c + k = b + c$ y $k \neq 0$, k que es un cierto número natural que al seguir la regla de simplificación es equipotente a la condición $a + k = b$ y $k \neq 0$ para un cierto k natural, dicho de otra manera, a la condición $a < b$.

Supóngase que $a < b$ y $c \neq 0$. Existe un tal número natural k para el cual $a + k = b, k \neq 0$. Multiplicando los dos elementos de la igualdad por c, se obtiene $ac + kc = bc$. Según el TEOREMA 2.15, $kc \neq 0$, ya que $k \neq 0$ y $c \neq 0$; así que, $ac < bc$. □

COROLARIO 3.9. *La relación $\leq$ es monótona con respecto a la adición y a la multiplicación, es decir que para cualquier a, b y c naturales se tiene:*

(1) $a \leq b$ si y solo si $a + c \leq b + c$:

(2) $si\ a \leq b$, entonces $ac \leq bc$.

TEOREMA 3.10. *Para cualquier número natural a, b y c de $ac < bc$ se deduce $a < b$.*

Demostración. Según el corolario 3.9 para cualquier a, b, c naturales

Si $b \leq a$, entonces $bc \leq ac$. De la ley de contraposición se demuestra la afirmación:

Si $ac < bc$, entonces $a < b$. □

Orden total de un conjunto de los números naturales.

TEOREMA 3.11. *El sistema $\langle \mathrm{N}, < \rangle$ es un conjunto bien ordenado.*

Demostración. Según el corolario 3.7 el sistema $\langle \mathrm{N}, < \rangle$ es un conjunto totalmente ordenado. Se debe demostrar que cualquier sub-conjunto no vacío del conjunto N de los números naturales posee el elemento más pequeño. Supóngase que existe un sub-conjunto no vacío A del conjunto N que no posee el elemento más un pequeño. Demuéstrese por recurrencia sobre la variable natural b que para cualquier b se confirma la fórmula

$A\,(b)\colon a \in A \longrightarrow b \leq a.$

Aparentemente, la fórmula se cumple para $b = c$, es decir que

$A\,(0)\colon a \in A \longrightarrow 0 \leq a$

Plantéese que para cualquier a y un cierto número natural n se confirma la fórmula
$A\,(n)$: $a \in A \longrightarrow n \leq a$
En ese caso $n \notin A$, puesto que en el contrario de los casos n sería el elemento más pequeño del conjunto A; así que, $a \in A \rightarrow n < a$. Dado que, según el TEOREMA 3.1, de $n < a$ se demuestra $n + 1 \leq a$, se tiene
$A(n+1)$: $a \in A \longrightarrow n + 1 \leq a$.
Por consiguiente, para cualquier n natural se confirma la implicación $A\,(n) \rightarrow A(n+1)$. Así se demuestra que la fórmula $A\,(b)$ es verdadera para cualquier b natural.

Por hipótesis, el conjunto A no es vacío y, por lo tanto, existe un elemento $m \in A \rightarrow m + 1 \leq m$. Ya que $m \in A$, se deduce que $m + 1 \leq m$, es decir que como resultado se tiene una contradicción. □

TEOREMA 3.12. Sea A un sub-conjunto del conjunto N de todos los números naturales. Si para cada número natural n se confirma la condición

(1) $(\forall m < n)(m \in A) \rightarrow n \in A$,

entonces $A = \mathrm{N}$.

Demostración. Plantéese que $A \neq \mathrm{N}$. En ese caso el conjunto $\mathrm{N} \setminus A$ no es vacío y (según el TEOREMA 3.11) posee un elemento más pequeño; existe entonces un número natural k que satisface a las condiciones:

(2) $k \in \mathrm{N} \setminus A$;

(3) $(\forall m < k)(m \in A)$.

En virtud de la condición (1) se tiene la implicación

(4) $(\forall m < k)(m \in A) \rightarrow k \in A$.

Según la regla de separación se deduce de (3) y (4) que $k \in A$, lo que, en virtud de (2), es imposible. □

TEOREMA 3.13. *Sea $A\,(x)$ un predicado singular cualquiera sobre un conjunto* N *de los números naturales. Si para cualquier número natural* $n(\forall m < k)\,A(m) \rightarrow A(n)$,
Entonces se tiene $A\,(x)$ para cualquier x natura.

La demostración del TEOREMA 3.13 se deduce sin duda del TEOREMA 3.12; dejamos a criterio del lector la reformulación.

Ejercicios

1. Demostrar que para todos los números naturales $a, b, c\ y\ d$:
(a) Si $a < b$ y $c < d$, entonces $a + c < b + d$;
(b) Si $a < b$ y $c < d$, entonces $a < b$ y $c < dc < bd$.
2. Demostrar que para cualquier número natural a_i, b_i si $a_1 < b_1, a_2 < b_2$, … $a_n < b_n$, se tiene $a_1 a_2 \ldots a_n < b_1 b_2 \ldots b_n$
3. Demostrar que para cualquier número natural a_i, b_i si $0 < a_1 \leq b_1, 0 < a_2 \leq b_2, \ldots, 0 < a_n \leq b_n$, se tiene
(1) $a_1 a_2 \ldots a_n \leq b_1 b_2 \ldots b_n$
Además, la igualdad en (1) tiene lugar si y solo si $a_1 = b_1, \ldots, a_n = b_n$.
4. Demostrar que para cualquier número natural a, b, y c se confirma la desigualdad $ab + bc + ca \leq a^2 + b^2 + c^2$.
5. Demostrar que para cualquier número natural a, b y $n > 1$ se confirma la desigualdad $(a + b)^n \leq 2^{n-1}(a^n + b^n)$.
6. Demostrar las desigualdades:
(a) $n^2 < 2^n$ para cualquier n natural si $n \geq 4$;
(b) $2^n < n!$ para cualquier n natural si $n \geq 4$;
(c) $n! < \left(\frac{n+1}{2}\right)^n$ para cualquier n natural si $n > 1$.
7. Demostrar por recurrencia sobre n la desigualdad de Bernoulli $(1 + a)^n \geq 1 + na$, donde a es un numero verdadero cualquiera superior a (-1).

§ 4. Anillo de Enteros

Grupo aditivo de enteros. Sea $\mathcal{N} =< \mathrm{N}, +, \cdot, 0, 1 >$ un sistema de números naturales. La operación de sustracción no siempre es posible en $\mathcal{N}$, dicho de otro modo, para los números naturales dados m y n la ecuación $m + x = n$ no siempre tiene solución en $\mathbb{N}$ con relación a x. Esto es solo cuando $m \leq n$ que la ecuación tiene una solución en $\mathbb{N}$ y además es única (según el TEOREMA 4.2.9); esta solución se denomina *diferencia entre los números n y m* y se escribe $n - m$.

Se trata de demostrar que existe un grupo aditivo abeliano $\mathcal{Z}$ que satisface las condiciones:

(1) El conjunto $\mathbb{N}$ se incluye en $|\mathcal{Z}|$ y la adición en el grupo $\mathcal{Z}$ es una prolongación de la adición en $\mathcal{N}$;

(2) La operación de sustracción en $\mathcal{Z}$ es siempre posible y cualquier elemento del grupo $\mathcal{Z}$ puede representarse bajo la forma de la diferencia de los números naturales.

Un grupo tal se denominara *grupo aditivo de enteros*.

TEOREMA 4.1. *Sea $\mathcal{N} =< \mathbb{N}, +, \cdot, 0, 1 >$ un sistema de números naturales. Existe un grupo abeliano $\mathcal{Z} =< \mathrm{Z}, +, - >$ que satisface las condiciones*:

(α) $\mathbb{N} \subset \mathrm{Z}$ y la suma de dos números naturales cualquiera m y n del grupo $\mathcal{Z}$ coincide con la suma de estos elementos de $\mathcal{N}$, es decir que $m + n = m + n$;

(β) para cualquier elemento a de Z existe números naturales n y m tal como $n + a = m$.

Demostración. Considérese el conjunto $\mathbb{N} \times \mathbb{N}$ pareja de números naturales. Defínase sobre este conjunto la relación binaria $\sim$ de la manera siguiente:

(1) $< m, n > \sim < r, s >$ si y solo si $m + s = r + n$.

Una verificación directa muestra que la relación $\sim$ es una relación de equivalencia sobre el conjunto $\mathbb{N} \times \mathbb{N}$.

Defínase sobre el conjunto de $\mathbb{N} \times \mathbb{N}$ la operación binaria $\oplus$ (adición) y la operación singular $\ominus$ por medio de las fórmulas

(2) $< m, n > \oplus < p, q > = < m + p, n + q >$;

(3) $\ominus < m, n > = < n, m >$.

La adición de pares es conmutativa y asociativa. Esta se deriva directamente de la conmutatividad y asosiatividad de la adición de números naturales.

Una verificación directa muestra que la equivalencia $\sim$ es una congruencia respecto a las operaciones $\oplus$ y $\ominus$, es decir que de

$< m, n > \sim < k, l >$ y $< p, q > \sim < r, s >$

quiere decir que

$< m, n > \oplus < p, q > \sim < k, l > \oplus < r, s >$

y de $< m, n > \sim < k, l >$ se deriva

$\ominus < m, n > \sim \ominus < k, l >$.

Nótese $[m, n]$ la clase de equivalencia que consta de la pareja $\langle m, n \rangle$. Según el TEOREMA 3.1 las operaciones $\oplus$, $\ominus$ (ver fórmulas (2) y (3)) se induce sobre el conjunto cociente $\mathbb{Z}_1 = \mathbb{N} \times \mathbb{N} / \sim$ las operaciones $+, -$:

(4) $[m, n] + [p, q] = [m + p, n + q]$;

(5) $-[m, n] = [n, m]$.

Conforme a (1) se obtiene

(6) $[m, n] = [r, s]$

Si y solo si $m + s = r + n$

El álgebra $\mathcal{Z}_1 =< \mathrm{Z}_1, +, - >$ es un grupo abeliano. De hecho, una verificación directa con la ayuda de las fórmulas (4)-(6) demuestra que la adición en $\mathbb{Z}_1$ es conmutativa y asociativa. El elemento $[0,0]$ es un elemento neutro en relación

a la adición en $\mathcal{Z}_1$, dado que conforme a (4) $[m,n]+[0,0]=[m,n]$. El elemento $-[m,n]$ es opuesto al elemento $[m,n]$, según (4) - (6)

$$[m,n]+(-[m,n])=[m,n]+[n,m]=$$
$$=[m+n,m+n]=[0,0].$$

Esto significa que el álgebra $\mathcal{Z}_1$ es un grupo abeliano.

Considérese el conjunto

$\mathbb{N}*=\{[0,k]\big|k\in\mathbb{N}\setminus\{0\}\}$.

La reunión de conjuntos $\mathbb{N}$ y $\mathbb{N}*$ se notará $\mathbb{Z}$:

$\mathbb{Z}=\mathbb{N}\cup\mathbb{N}*$.

Defínase la función h del conjunto Z_1 sobre $\mathbb{Z}$ de la manera siguiente:

$h([m+k,m])=k$ para cualquier k de $\mathbb{N}$;

$h([n,m+k])=[n,n+k]$ para cualquier k de $\mathbb{N}\setminus\{0\}$.

Se constata sin duda que h es una aplicación inyectiva del conjunto Z_1 sobre $\mathbb{Z}$. Existe entonces una función inversa h^{-1}, función inyectiva del conjunto $\mathbb{Z}$ sobre Z_1 que satisface las condiciones

$h\circ h^{-1}=\iota_z, h^{-1}\circ \mathrm{h}=\iota_{z_1}$,

Donde ι_z y ι_{z_1} son funciones idénticas de $\mathbb{Z}$ y Z_1 respectivamente.

Defínase la adición en $\mathbb{Z}$ para cualquier a,b de $\mathbb{Z}$ para ayudar a la fórmula

(I) $\quad a+b=h\left(h^{-1}(a)+h^{-1}(b)\right)$,

En cuanto a la operación simple, se definirá por la fórmula

(II) $\quad -a=h\left(-h^{-1}(a)\right)$.

De las fórmulas (I) y (II) se deducen las fórmulas

(III) $\quad h^{-1}(a+b)=h^{-1}(a)+h^{-1}(b)$,

(IV) $\quad h^{-1}(-a)=-h^{-1}(a)$.

Considérese que el álgebra $\mathcal{Z}=<\mathbb{Z},+,->$. Conforme a (III) y (IV) el álgebra $\mathcal{Z}$ es isomorfo en el grupo abeliano $\mathcal{Z}_1$. Quiere decir que el álgebra $\mathcal{Z}$ es un grupo abeliano. De hecho, la adición en $\mathcal{Z}$ es conmutativa, ya que, conforme a (I) y a la conmutativa de la adición en $\mathcal{Z}_1$, se obtiene

$$a+b=h\left(h^{-1}(a)+h^{-1}(b)\right)=h\left(h^{-1}(b)+h^{-1}(a)\right)=b+a.$$

La adición en $\mathcal{Z}$ es asociativa, dado que conforme a (I) y (II),

Se obtiene

$$a+(b+c)=h(h^{-1}(a)+h^{-1}(b+c))=h\left(h^{-1}(a)+h^{-1}(b)+h^{-1}(c)\right)=h\left(h^{-1}(a+b)+h^{-1}(c)\right)=(a+b)+c.$$

El número natural 0 es un elemento neutro con relación a la adición en $\mathcal{Z}$ ya que para cualquier a de $\mathbb{Z}$ se tiene

$$a+0=h\left(h^{-1}(a)+h^{-1}(0)\right)=h(h^{-1}(a)+[0,0])=$$
$$=h\left(h^{-1}(a)\right)=a$$

Para cualquier a de $\mathbb{Z}$ se verifica la igualdad $a+(-a)=0$, dado que $a+(-a)=h\left(h^{-1}(a)+h^{-1}(-a)\right)=$

$$=h\left(h^{-1}(a)+(-h^{-1}(a)\right)=h([0,0])=0.$$

Entonces, el álgebra $\mathcal{Z}$ es un grupo abeliano.

Muéstrese que la condición $(\propto)$es verdadera. De hecho, conforme a (I) para cualquier m,n de $\mathbb{N}$, se tiene

$m+n=h\big(h^{-1}(m)+h^{-1}(n)\big)=h([m,0]+[n,0])=$

$$=h([m+n,0])=m+n,$$

Dicho de otro modo, la adición en $\mathcal{Z}$ prolonga la adicion en $\mathcal{N}$.

Muéstrese que la condición (β) es verdadera. Sean a un elemento cualquiera de $\mathbb{Z}$ y $h^{-1}(a)=[m,n]$; en ese caso

$n+a=h\big(h^{-1}(n)+h^{-1}(a)\big)=$

$$=h([n,0]+[m,n])=$$

$=h([n+m,n])=m$, es decir que $n+a=m$.

Como resultado, cualquier elemento de $\mathbb{Z}$ puede representarse bajo la forma de una diferencia de números naturales: $a=m-n$.

En resumen, se estableció que el álgebra $\mathcal{Z}=<\mathbb{Z},+,->$ es un grupo abeliano que satisface a las condiciones $(\propto)$ y (β). □

DEFINICIÓN. Se denomina *grupo aditivo de enteros* al grupo abeliano $\mathcal{Z}=<\mathbb{Z},+,->$ que satisface las condiciones $(\propto)$ y (β) del TEOREMA 4.1.

Multiplicación natural en un grupo aditivo de enteros. Sea $\mathcal{Z}_+=<,+,->$ un grupo aditivo de enteros. Según el TEOREMA 4.1, $\mathbb{N}\subset\mathbb{Z}$ y cualquier elemento de $\mathbb{Z}$ puede representarse bajo la forma de una diferencia de números naturales; entonces,

$\mathbb{Z}=\{m-n|m,\ n\in\mathbb{N}\}$.

Defínase la multiplicación en el grupo $\mathcal{Z}_+$ de la manera siguiente: para cualquier elemento $m-n$ y $p-q$ de $\mathbb{Z}$ se plantea

(1) $(m-n)\cdot(p-q)=(mp+nq)-(mq+np)$,

Donde $m,n,p,q,\in\mathbb{N}$ y mp,nq,mq,np son productos de los números naturales en el sistema $\mathcal{N}$.

Represéntese cualquier elemento de $\mathbb{Z}$ bajo la forma de una diferencia de números naturales de manera no univoca. Entonces, es necesario verificar que el producto de enteros definido por la fórmula (1) es independiente de su representación bajo la forma de una diferencia de números naturales. Muéstrese que para cualquier elemento $p-q$ del conjunto $\mathbb{Z}$ de la igualdad

(2) $m-n=m'-n'\ \ (m,n,\ m',n'\in\mathrm{N})$

Resulta la igualdad

(3) $(m'-n')\cdot(p-q)=(m-n)\cdot(p-q)$.

De hecho, por definición (1),

$(m'-n')(p-q)=(m'p+n'q)-(m'q+n'p)$.

Según (1) es (4) basta con verificar que

(4) $(mp+nq)+(m'q+n'p)=(m'p+n'q)+(mq+np)$,

ó

(5) $(m+n')p+(n+m')q=(m'+n)p+(n'+m)q$.

Debido a (2) $m+n'=m'+n$. Entonces, las igualdades (5), (4) y (3) son verdaderas.

Una verificación directa de naturaleza simple muestra que para cualquiera de los elementos $m-n$ y $p-q$ del conjunto $\mathbb{Z}$ de las igualdades

$m-n=m'-n'$ y $p-q=p'-q'$

Resulta la igualdad

$(m' - n') \cdot (p' - q') = (m - n)(p - q)$.

En resumen, se ha establecido que una multiplicación en el grupo $\mathcal{Z}_+$ definido por la fórmula (1) es independiente del modo de representación de los factores bajo la forma de diferencia de números naturales.

DEFINICIÓN. La multiplicación en un grupo aditivo de enteros $\mathcal{Z}_+$ definido por la fórmula (1) es llamada *multiplicación natural*.

Anillo de enteros. Para empezar se da la definición.

DEFINICIÓN. El anillo $\mathcal{K}$se denomina *anillo de enteros* si el grupo aditivo del anillo $\mathcal{K}$ es un grupo aditivo de enteros y la multiplicación en el anillo $\mathcal{K}$ es conmutativa y prolonga la multiplicación de los números naturales (en el sistema $\mathcal{N}$ de números naturales).

THEOREMA 4.2. Sean $\mathbb{Z}, < +, - >$, *un grupo aditivo de enteros, una multiplicación natural en ese grupo y 1 la unidad del sistema* N *de números naturales. En ese caso el álgebra* $\mathcal{Z} =< \mathbb{Z}, +, -, \cdot, 1 >$ *es un anillo de enteros.*

Demostración. Muéstrese que el álgebra $\mathcal{Z}$ es un anillo conmutativo. Por hipótesis, el álgebra $< \mathbb{Z}, +, - >$, grupo aditivo del anillo, es un grupo abeliano, puesto que es un grupo aditivo de enteros.

Sean a, b, c elementos arbitrarios del conjunto $\mathbb{Z}$. Según el TEOREMA 4.1 se pueden representar bajo la forma de la diferencia de los números naturales. Plantéese

(1) $a = m - n,\ b = p - q,\ c = r - s\ \ (m, n, p, q, r, s\ \in \mathbb{N})$.

Una multiplicación natural en $\mathbb{Z}$ se define por la fórmula

(2) $a \cdot b = (m - n) \cdot (p - q) = (mp + nq) - (mq + np)$.

Una multiplicación natural es conmutativa, porque

$b \cdot a = (p - q) \cdot (m - n) = (pm + qn) - (pn + qm)$,

del mismo modo son conmutativas la adición y multiplicación de números naturales.

Una multiplicación natural es asociativa. Efectivamente, conforme a (1) y (2), se obtiene:

$a \cdot (b \cdot c) = (m - n)[(p - q)(r - s)] =$

$= (m - n)[(pr + qs) - (ps + qr)] =$

$= (mpr + mqs + nps + nqr) -$

$-(mps + mqr + nqr + nqs)$;

$(a \cdot b) \cdot c = [(m - n)(p - q)](r - s) =$

$= [(mp + nq) - (mq + np)](r - s) =$

$= (mpr + nqr + mqs + nps) -$

$-(mps + nqs + mqr + npr)$.

Como resultado, conforme a la conmutatividad de la adición de números naturales $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

El elemento 1 es un elemento neutro respecto a la multiplicación natural. De hecho, para cualquier a de $\mathbb{Z}$, se obtiene

$a \cdot 1 = (m - n)(1 - 0) = m \cdot 1 = m - n = a$.

Entonces, el álgebra $< \mathbb{Z}, \cdot, 1 >$ es un monoide conmutativo.

La multiplicación natural es distributiva respecto a la adición. De hecho,

$(a + b) \cdot = [(m + p) - (n + q)](r - s) =$

$= (mr + pr + ns + qs) - (ms + ps + nr + qr)$;

$$ac + bc = [(mr + ns) - (ms + nr)] + [(pr + qs) - (ps + qr)] =$$
$$= (mr + ns + pr + qs) - (ms + nr + ps + qr).$$

Como resultado, $(a + b) \cdot c = a \cdot c + b \cdot c$. Dado que la multiplicación natural es igualmente conmutativa, se tiene del mismo modo la igualdad $c(a + b) = ca + cb$.

En resumen, se estableció que el álgebra $\mathcal{Z}$ es un anillo conmutativo.

La multiplicación natural prolonga la multiplicación de los números naturales en el sistema $\mathcal{N} =< \mathbb{N}, +, \cdot, 0, 1 >$. De hecho, para m y n de $\mathbb{N}$, se tiene

$m \cdot n = (m - 0)(n - 0) = (m \cdot n + 0 \cdot 0) - (m \cdot 0 + n \cdot 0) = m \cdot n.$

Además, por hipótesis, el grupo aditivo del anillo $\mathcal{Z}$ es un grupo aditivo de enteros. Como resultado, el anillo $\mathcal{Z}$es un anillo de enteros.□

DEFINICIÓN. Si para dos enteros a y b existe un número natural k tal como $a + k = b$ y $k \neq 0$, se dice entonces que ≪ a es inferior a b ≫ y se escribe $a \leq b$ si $a < b$ o $a = b$.

La relación inversa de $<$ se denota por el símbolo$>$. Entonces, $a > b$ si y solo si $b < a$.

TEOREMA 4.3. Sea $\mathcal{Z} =< \mathbb{Z}, +, -, \cdot, 1 >$ *un anillo de enteros*.

Se obtiene entonces

(1) Para cualquier entero a y b se satisface una y solo una de las tres condiciones: $a < b, a = b, b < a$;

(2) Para cualquier entero a se satisface una y solo una de las tres condiciones: $a < 0, a = 0, 0 < a$;

(3) La relación $<$ es monótona en relación a la adición, es decir, para cualquiera de los enteros $a, b,$ y c $a < b$ si y solo si $a + c < b + c$;

(4) La relación $<$ es monótona en relación a la multiplicación , es decir, para cualquiera de los enteros $a, b, y\ c$ Si $a < b\ y\ c > 0$, se tiene $ac < bc$.

La demostración de este TEOREMA se deja a opción del lector.

TEOREMA de la división con resta. Sean a un entero y b un número natural diferente de cero. Dividir a por b con la resta se representa bajo la forma $a = bq + r$, donde $0 \leq r < b, q\ y\ r$ son los enteros. q es en ese caso llamado *cociente entero*, mientras que r es la *resta* de la división de a por b.

Una división con resta siempre es posible, mientras que el cociente incompleto (entero) y la resta son definidos de manera univoca por el número dividido (dividendo) y el divisor como lo muestra el TEOREMA siguiente.

TEOREMA 4.4*. Para cualquiera de los enteros a, b para $b > 0$ tan solo existe una pareja de enteros q y r que satisfacen a las condiciones:*

(1) $a = bq + r$ y $0 \leq r < b$.

Demostración. Demuéstrese que existe al menos una pareja de números q, r que satisfacen las condiciones (1). Primero, consideramos el caso donde a es un número natural. Fíjese b y demuéstrese por recurrencia sobre a que

(2) Existe una pareja de enteros q, r que satisface a (1).

Para $a = 0$ la afirmación (2) es verdadera, ya que $0 = b \cdot 0 + 0$. Admítase que (2) es verdadera para $a = n$, es decir que existe los enteros q, r tales como

(3) $n = bq + r$ y $0 \leq r < b$,

Y demuéstrese que es verdadera para $a = n + 1$. Quiere decir que (3) $n + 1 = bq + (r + 1)$ y $0 < r + 1 \leq b$. Si $r + 1 < b$ la pareja de números $q, r + 1$ es precisamente la pareja que se busca. Si, por el contrario, $r + 1 = b$, entonces $n + 1 = b(q + 1)$ y la pareja de números $q + 1, 0$ es la pareja que se busca.

Ahora considérese el caso donde $a < 0$; se tiene entonces$-a > 0$. Conforme a la demostración antes mencionada, existe para la pareja de números – a, b de los enteros q', r' tales como $-a = bq' + r'$ y $0 \leq r' < b$. Si $r' = 0, a = (b - q') + 0$. Si, por el contrario, $r' > 0$, entonces $a = b(-q' - 1) + (b - r')\ y\ 0 < b - r' < b$.

Planteando $q = -q' - 1$ y $r = b - r'$, se obtiene
$a = bq + r$ y $0 < r < b$.

En resumen, se demostró que para cualquiera de los enteros a, b para $b > 0$, existe al menos una pareja de enteros q, r que satisface las condiciones (1).

Falta demostrar que la pareja de enteros que satisface las condiciones (1) es única. Supóngase que para el entero a se tiene dos representaciones:

(4) $a = bq + r, \qquad 0 \leq r < b;$
(5) $a = bq_1 + r_1, \qquad 0 \leq r_1 < b.$

Plantéese que $r \neq r_1$. Entonces, $r > r_1$ ó $r_1 > r$. Si $r > r_1$, conforme a (4) y (5), se tiene

(6) $0 < r - r_1 < b;$
(7) $r - r_1 - b(q_1 - q).$

De (6) y (7) se deduce que $q_1 - q > 0$ y, como resultado, $q_1 - q \geq 1$. De lo anterior, conforme a (7), se deriva la desigualdad $r - r_1 \geq b$ que contradice (6). Compruébese de manera análoga que igualmente es imposible en el caso de $r_1 > r$. Por consiguiente, $r = r_1$ y, conforme a (4), (5), $b(q - q_1) = 0$. Como $b \neq 0$, se tiene: $q - q_1 = 0$ y $q = q_1$. □

Relación de divisibilidad en un anillo de enteros. Estúdiese las propiedades más simples de la divisibilidad en un anillo de enteros.

DEFINICIÓN. Sean a y b enteros. Se dice que b divide a a si $a = bq$ para cierto entero q. En lugar de que≪ b divida a $a \gg$ se dice también que a es divisible por b, o que a es un múltiplo de b y se escribe $b|a$ ó $a \vdots b$. En caso contrario se dice que *a no se divide por b, a no es un múltiplo de b, b no se divide por a, b no es un divisor de a* y se escribe $b \nmid a$.

TEOREMA 4.5. *Sean a, b, c, d, m, n cualquier entero*.
Entonces se tiene:

(1) $a|a;$
(2) $a|0;$
(3) $si\ 0|a, entonces\ a = 0;$
(4) $\pm 1|a;$
(5) $si\ a|b\ y\ b|c, entonces\ a|c, es\ decir\ que\ la\ relación\ de\ divisibilidad\ es\ transitiva;$
(6) $si\ c|a, entonces\ c|ab;$
(7) $si\ c|a\ y\ c|b, entonces\ c|(a \pm b);$
(8) $si\ b|a, entonces\ bc|ac;$
(9) $si\ c \neq 0, entonces\ de\ bc|ac\ se\ deduce\ b\ |a;$
(10) $si\ a|c\ y\ b|d, entonces\ ab|cd;$
(11) $si\ a\ |b \quad y \quad a|c, \quad entonces \quad a|(mb + nc).$

Las propiedades (1)-(11) de la relación de divisibilidad fácilmente se deducen de la definición de la divisibilidad y de las propiedades del anillo $\mathcal{Z}$. La demostración se deja al criterio del lector.

Lema 4.6. *Si el producto ab de números naturales es igual a la unidad, se tiene entonces $a = b = 1$.*

Demostración. De la hipótesis $ab = 1$ se deduce que a y b son diferentes de cero. Según el TEOREMA 2.6 pueden representarse bajo la forma de $a = c + 1, b = d + 1$. Entonces, $ab = cd + c + d + 1 = 1$ y $cd + c + d = 0$. Si la suma de los números naturales es nula, significa que conforme al corolario 2.8, cada término de la suma es nulo. En particular, $c = d = 0$; así que, $a = b = 1$. □

TEOREMA 4.7. *Si un entero a divide la unidad, a es entonces igual a ± 1.*

Demostración. Plantéese que a divide la unidad, es decir que $ab = 1$ para cierto entero b. Entonces $a^2b^2 = 1$. a^2 y b^2 siendo números naturales, según el lema 4.6 se tiene entonces $a^2 = 1$. Por consiguiente, según el TEOREMA 4.1, se obtiene

(1) $a = \pm b$.

Ya que a o $-a$ son números naturales, según el lema 4.6, se deduce de $a^2 = 1$ y de la igualdad (1) que $a = 1$, o $-a = 1$. □

TEOREMA 4.8. *Si los enteros a y b se asocian (es decir a| y b|a),* entonces $a = \pm b$.

Demostración. Por hipótesis, a divide b y b divide a, es decir $b = ac$ y $a = bd$ para los enteros *c* y d, entonces,

(1) $a = acd$.

Si $a = 0$, entonces $b = 0 \cdot c = 0$, y el TEOREMA se verifica. Si $a \neq 0$, se deduce de (1) que $cd = 1$. Según el TEOREMA 4.7 de la igualdad $cd = 1$ se dedujo que $d = \pm 1$. Además, $a = bd$; entonces, $a = \pm b$. □

Ejercicios.

1. Sea $m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$, donde m es un número natural. Mostrar que para $m \neq 0$ existe una aplicación inyectiva del conjunto $\mathbb{Z}$ sobre $m\mathbb{Z}$.
2. Sea $\mathcal{Z}' = \langle \mathbb{Z}, +, - \rangle$ un grupo aditivo de enteros. Mostrar que el conjunto $m\mathbb{Z}$, donde m es un entero, es cerrado en el grupo $\mathcal{Z}$, es decir cerrado respecto a las operaciones $+$ y $-$.
3. Mostrar que un conjunto no vacío de enteros cerrado en relación a la suma no son obligatoriamente compuestos de múltiplos de un entero fijo.
4. Mostrar que un conjunto no vacío de enteros cerrado en el grupo $\mathcal{Z}$ (cerrado respecto a las operaciones $+$ y$-$) está compuesto de múltiplos de cierto entero fijo.
5. Establecer si, en el grupo aditivo de enteros, están los subgrupos respecto a las operaciones $+, -$ los conjuntos de enteros siguientes:
   (a) El conjunto de todos los números pares;
   (b) El conjunto de los números naturales;
   (c) El conjunto de los números impares.
6. Sean $\mathcal{Z} = \langle \mathbb{Z}, +, - \rangle$ y m un entero fijo. Mostrar que el álgebra $m\mathcal{Z} = \langle m\mathbb{Z}, +, - \rangle$ es un subgrupo del grupo $\mathcal{Z}$. Mostrar que cualquier subgrupo del grupo $\mathcal{Z}$ coincide con el grupo $m\mathcal{Z}$ para cierto m natural.
7. Demostrar que un grupo aditivo de enteros $\mathcal{Z}$ es isomorfo en el subgrupo $m\mathcal{Z}$ para cualquier entero m diferente de cero.
8. Mostrar que el anillo $\mathcal{Z}$ de enteros no tiene automorfismo diferente del anillo identidad.
9. Demostrar que el anillo $\mathcal{Z}$de enteros no tiene un sub-anillo diferente de $\mathcal{Z}$.
10. Sea $\mathcal{K}$ un anillo cualquiera. Demostrar que en el anillo $\mathcal{K}$ no existe más que un único homomorfismo en el anillo $\mathcal{Z}$de enteros.
11. Sea $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} | m, n \in \mathbb{Z}\}$. Demostrar que el álgebra $\mathcal{Z}[\sqrt{2}] = \langle \mathbb{Z}[\sqrt{2},], +, -, \cdot, 1 \rangle$ del tipo $(2, 1, 2, 0)$, donde $+, -, \cdot$son operaciones banales sobre los números reales, es un anillo conmutativo. Indicar un automorfismo no trivial de este anillo.
12. Demostrar que no existe el homomorfismo del anillo $\mathcal{Z}[\sqrt{2}]$ en el anillo $\mathcal{Z}\sqrt{3}$ y que estos anillos no son isomorfos.
13. Sea $\mathcal{K} = \{\langle a, b \rangle | a, b \in \mathbb{Z}\}$, las operaciones $+, -, \cdot, e$ sobre el conjunto $\mathcal{K}$ siendo definidos de la manera siguiente:
    $\langle a, b \rangle + \langle c, d \rangle = \langle a + c, b + d \rangle$;
    $-\langle a, b \rangle = \langle -a, -b \rangle$;
    $\langle a, b \rangle \cdot \langle c, d \rangle = \langle ac, bd \rangle$;
    $e = \langle 1, 1 \rangle$.

Mostrar que el álgebra $\langle \mathrm{K}, +, -, \cdot, e \rangle$ es un anillo conmutativo con divisores de cero.

14. Demostrar que para cualquier n natural:
    (a) $5^{2n} - 1$ es divisible por 24;

(b) $4^n + 6_n - 1$ es divisible por 9;
(c) $10^{n3} - 1$ es divisible por 3^3;
(d) $3^{2n} + 5$ no es divisible por 8.

15. Demostrar que el producto de tres enteros consecutivos cualquiera se dividen por 6.
16. Demostrar que para cualquier entero n:
(a) $n^3 - n$ es divisible por 3;
(b) $n^5 - n$ es divisible por 5;
(c) $n^7 - n$ es divisible por 7;
(d) $n\ (n^2 + 5)$ es divisible por 6;
(e) $n^5 - n$ es divisible por 30.
17. Mostrar que si un entero n no es divisible por 7, $n^3 - 1$ ó $n^3 + 1$ lo son.
18. Demostrar que para cualquier entero a y b:
(1) Si $a|b$ y $b \neq 0,$ entonces $|a| \leq |b|$,
(2) Si $a|b$ y $|b| < |a|$, entonces $b = 0$.
19. Demostrar que para cualquier entero a y b
$|ab| = |a| \cdot |b|,$ $|a + b| \leq |a| + |b|.$
20. Demostrar por recurrencia sobre n que para cualquier enteros $a_1, \dots, a_n$ se tiene la desigualdad $a_1^2 + \dots + a_n^2 > 0$, excepto el caso donde $a_1 = \cdots = a_n = 0$.
21. Demostrar que cualquier conjunto no vacío de enteros limitados inferiores (superiores) tiene un mínimo (un máximo) elemento.
22. Demostrar que para cualquier entero a y cualquier entero positivo b existe un entero único n tal como $nb \leq a < (n + 1)b$.
23. Demostrar la generalización siguiente del TEOREMA de división con la resta: para cualquiera de los enteros a y b con $b \neq 0$ existe una pareja única de enteros q, r por la cual $a = bq + r$ y $0 \leq r < |b|$.

§5. Cuerpos. Cuerpos de los números racionales

Noción de los cuerpos. Deseen las principales DEFINICIÓNes.

DEFINICIÓN. El elemento a del anillo $\mathcal{K}$ se denomina *elemento invertible del anillo* si existe en el anillo un elemento b tal como $ab = ba = 1_{\mathcal{K}}$. Además, los elementos a y b son llamados *mutuamente inversos*.

DEFINICIÓN. Se denominan cuerpos a un anillo conmutativo en el cual el cero es diferente de la unidad, $0_{\mathcal{K}} \neq 1_{\mathcal{K}}$y cada elemento no nulo es un elemento invertible del anillo.

DEFINICIÓN. Sea $\mathcal{F}, = \langle F, +, -, \cdot, 1\rangle$ un cuerpo. El grupo $\langle F, +, -\rangle$ se denomina *grupo aditivo de un cuerpo*. Su elemento neutro se denomina *cero del cuerpo* y se nota por el símbolo 0 ó $0_{\mathcal{F}}$.

El elemento 1, elemento neutro en relación a la multiplicación, es la *unidad del cuerpo* y se nota igualmente por el símbolo $1_{\mathcal{F}}$.

DEFINICIÓN. Se denomina *sub-cuerpo de un cuerpo* $\mathcal{F}$ un sub-anillo del cuerpo $\mathcal{F}$ en el cual cualquier elemento no nulo es inversible. El sub-cuerpo del cuerpo $\mathcal{F}$ diferente de $\mathcal{F}$ se denomina *sub-cuerpo propio.* Está claro que cualquier sub-cuerpo es un cuerpo.

DEFINICIÓN. Un cuerpo es llama *simple* si este no tiene sub-cuerpos propios.

Propiedades fundamentales de un cuerpo. Sean a, b los elementos del cuerpo $\mathcal{F}$ y $b \neq 0$. La ecuación $bx = a$ tiene en el cuerpo la solución ab^1; se verifica, sin duda que ab^{-1} es la solución única a la ecuación. El elemento ab^{-1} se denota por el símbolo $\frac{a}{b}$ o a/b.

TEOREMA 5.1. *Sea* $\mathcal{F} = \langle F, +, -, \cdot, 1\rangle$ *un cuerpo. Entonces se tiene para cualquier elemento* a, b, c *del cuerpo:*

(1) Si $ab = 1$, entonces $a \neq 0$ y $b = a^{-1}$

(2) Si $ac = bc$ y $c \neq 0$, entonces $a = b$;

(3) Si $ab = 0$, entonces 0 o $b = 0$;

(4) Si $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$;

(5) $\frac{a}{b} = \frac{c}{d}$ $si\ y\ solo\ si\ ad = bc, b \neq 0\ y\ d \neq 0$;

(6) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bc}$;

(7) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

(8) $\frac{a}{b} + \frac{(-a)}{b} = 0\ y\ -\left(\frac{a}{b}\right) = \frac{-a}{b}$;

(9) $si\ a \neq 0\ y\ b \neq 0, entonces\ \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$;

(10)$\frac{ac}{bc} = \frac{a}{b}$.

Demostración. (1) Sí $ab = 1$, entonces $a \neq 0$, ya que con $a = 0\ 0 \cdot b = 1$ y $0 = 1$, lo que no es posible en un cuerpo. Puesto que $a \neq 0$, existe un elemento a^{-1} inverso de a y $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}1 = a^{-1}$.

(2) Si $ac = bc\ y\ c \neq 0$, existe un elemento c^{-1} en el cuerpo y $a = (ac)c^{-1} = (bc)c^{-1} = b$, es decir $a = b$.

(3) A partir de $ab = 0$ se deduce $a = 0$o $b = 0$. En efecto, si $a \neq 0$, existe un elemento a^{-1} y $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

(4) Al Seguir la ley de contraposición de (3) se deduce que $\urcorner(a = 0 \vee b = 0) \rightarrow \urcorner(ab = 0)$, es decir que $(a \neq 0 \wedge b \neq 0) \rightarrow (ab \neq 0)$.

(5) Sea $a/b = c/d$, es decir $ab^{-1} = cd^{-1}$. Entonces se obtiene $b \neq 0, d \neq 0$ y $ad = (ab^{-1})(bd) = cb^{-1} \cdot bd = cb$ es decir $ad = cb$. Recíprocamente: de la igualdad $ad = cb$ con $b \neq 0, d \neq 0$ se deducen las igualdades $adb^{-1}ad^{-1} = cbb^{-1}d^{-1}$ y $ab^{-1} = cd^{-1}$.

(6) Dado que $a/b = ab^{-1}$ y $c/d = cd^{-1,}$ se tiene $\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1} = add^{-1}b^{-1} \pm cbb^{-1}d^{-1}(ad \pm bc)(bd^{-1}) = (ad \pm bc)/bd$.

(7) Para $b \neq 0$ y $d \neq 0$

$\frac{a}{b}\frac{c}{d} = ab^{-1}cd^{-1} = ac\ (bd) = \frac{ac}{bd}$.

(8) Para $b \neq 0$

$\frac{a}{b} + \frac{(-a)}{b} = ab^{-1} + (-a)b^{-1} = (a - a)b^{-1} = 0$,

Entonces, $-(a/b) = -a/b$

(9) Si $a \neq 0$ y $b \neq 0$, entonces $(a/b)^{-1} = (ab^{-1})^{-1} = ba^{-1} = b/a$.

(10) Para $b \neq 0$ y $c \neq 0$

$ac/bc = ac\ (bc) = acc^{-1}b^{-1} = ab^{-1} = a/b$. □

Cuerpo de números racionales. Introdúzcase la noción de cuerpos fraccionarios (los cocientes) del campo de integridad.

DEFINICIÓN. Plantéese que $\mathcal{F}$ se denomina *cuerpos fraccionarios en el campo de integridad* $\mathcal{K}$ si satisfacen las condiciones:

($\propto$) $\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{F}$

(β) Para cualquier x de F existen elementos a, b, del anillo $\mathcal{K}$ tales como $x = ab^{-1}$.

TEOREMA 5.2. *Para cualquier campo de integridad $\mathcal{K}$ se tiene un cuerpo de fracciones. Si $\mathcal{F}$ y $\mathcal{T}$ son cuerpos de fracciones de un anillo $\mathcal{K}$, se tiene un isomorfismo del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{T}$ pasando del mismo modo cada elemento del anillo $\mathcal{K}$.*

La demostración de este TEOREMA se explica en el capítulo XIII (véase los TEOREMAs 13.21 y 13.2).

El anillo $\mathcal{Z}$ de enteros es un dominio de integridad. Como resultado, según el TEOREMA 5.2, existe para el anillo $\mathcal{Z}$ un cuerpo de fracciones y cualquier par de fracciones del anillo $\mathcal{Z}$ son isomorfas.

DEFINICIÓN. Denomínese *cuerpo de número racionales* a un cuerpo de fracciones de un anillo de enteros. Los elementos del cuerpo de los *números racionales* son los números racionales.

Lo que se obtiene de la definición que cualquier número racional puede representarse bajo la forma de un cociente de dos enteros.

Nótese que cualquier cuerpo isomorfo en un cuerpo de números racionales es también un cuerpo de números racionales.

La relación de orden sobre el conjunto Q de números racionales se introduce en medio de la relación del orden $<$ sobre el conjunto $\mathbb{Z}$ de enteros.

DEFINICIÓN. *La relación del orden $<$ sobre el conjunto Q* de números racionales se define de la manera siguiente: para dos números racionales cualquieras $p/q\ y\ r/s$, donde $p, r\ \in \mathbb{Z}$ y $q, s\ \in\ \mathbb{N}\ \setminus \{0\}, \frac{p}{q} < \frac{r}{s}$ si y solo si $ps\ < qr$.

Es fácil verificar que $<$ sobre el conjunto Q de números racionales es una relación de orden estricta que prolonga la relación de orden sobre el conjunto $\mathbb{Z}$ de enteros.

TEOREMA 5.3*. La relación binaria $<$ sobre el conjunto Q de números racionales es dada por las propiedades siguientes:*

(1) Para cualquier a, b, c de Q si $a\ < b$ y $b < c$, entonces $a < c$;

(2) Para cualquier a, b de Q no existe más que una de tres relaciones $a < b,\ a = b,\ b < a$;

(3) *Para cualquier a, b, c de Q si $a < b,$ entonces $a + c < b + c$;*

(4) *Para cualquier a, b, c de Q si $a < b\ y\ 0 < c$, entonces $ac < bc$.*

La demostración del TEOREMA se deja al criterio del lector.

Ejercicios

1. Establecer aquellos conjuntos siguientes de números reales que constituyen cuerpos relativamente en las operaciones triviales $+, -,\ \cdot$ sobre estos conjuntos:

(a) Todos los números naturales;

(b) Todos los números racionales en denominadores impares;

(c) Todos los números del aspecto $a + b\sqrt{2},\ a\ y\ b$ que son racionales;

(d) Todos los números del aspecto $a + b\sqrt{5},\ a\ y\ b$ que son racionales;

(e) Todos los números del aspecto $a + b\ \sqrt[3]{2}, a\ y\ b$ que son racionales;

(f) Todos los números del aspecto $a\ + b\ + \sqrt[3]{2}\ + c\sqrt[3]{4},\ a, b$ y que son racionales.

2. Sea $\mathcal{K}$ un conjunto de todas las matrices de la forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ para a y b racionales. Demostrar que el álgebra $< K, +, -, \cdot, e >$, donde $+, -, \cdot$ son operaciones sobre las matrices y $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, es un cuerpo. Mostrar que ese cuerpo consta de un elemento x tal como $x^2 = -e$.

3. Sea F un conjunto de todas las matrices de la forma $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ para a y b racionales. Demostrar que el álgebra $\mathcal{F} =< F, +, -, \cdot, e >$, donde $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, es un cuerpo. Mostrar que la aplicación $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \longmapsto a + b\sqrt{2}$ es un isomorfismo del cuerpo $\mathcal{F}$ sobre el cuerpo $Q(\sqrt{2})$.
4. ¿Cuáles de los anillos $Z_2, Z_3, Z_4, Z_5 y\ Z_6$ son cuerpos?
5. Demostrar que un cuerpo es desprovisto de los divisores de cero.
6. Mostrar que cada sub-anillo de un cuerpo es un dominio de integridad.
7. Sea a un elemento no nulo de un cuerpo. Demostrar que para cualquier entero m y n las igualdades $a^{m+n} = a^m a^n$ y $(a^m)^n = a^{mn}$ son satisfechas.
8. Sean a, b y c los elementos cualquieras de un cuerpo $\mathcal{F}$. Demostrar que de la igualdad $ab = ac$ se obtiene $b = c$ si y solo si$a \neq 0$.
9. Demostrar que la intersección de cualquier grupo de sub-cuerpos $\mathcal{F}$ es un sub-cuerpo del cuerpo de $\mathcal{F}$
10. Demostrar que cualquier dominio de integridad finito es un cuerpo.
11. Mostrar que el cuerpo Q de los números racionales no tiene sub-cuerpos diferentes de Q.
12. Demostrar que cualquier sub-cuerpo del cuerpo $Q(\sqrt{2})$ ya sea Q, o $Q(\sqrt{2})$.
13. Describir todos los sub-anillos del cuerpo Q de los números racionales.
14. Sea $\varphi: \mathcal{F} \to \mathcal{F}'$ un homomorfismo del anillo del cuerpo $\mathcal{F}$ en el cuerpo $\mathcal{F}'$. Mostrar que con la aplicación φ la imagen del cuerpo $\mathcal{F}$ es un sub-cuerpo del cuerpo $\mathcal{F}'$.
15. Demostrar que un homomorfismo del anillo del cuerpo $\mathcal{F}$ ya sea una aplicación de cero, o un isomorfismo del cuerpo $\mathcal{F}$ sobre su imagen.
16. Sea $\varphi: \mathcal{F} \longrightarrow \mathcal{F}'$ un homomorfismo del anillo. Si $\mathcal{F}$ es un cuerpo, $a, b, \in F$ y $b \neq 0$, se tiene $\varphi(a/b) = \frac{\varphi(a)}{\varphi(b)}$; demostrarlo.
17. Demostrar que una aplicación idéntica es el único automorfismos del cuerpo Q de los números racionales.
18. Mostrar que cualquier cuerpo compuesto de dos elementos es isomorfo en el cuerpo Z_2.
19. Demostrar que un anillo isomorfo en un cuerpo es el mismo cuerpo.
20. Mostrar que no existe homomorfismo en el anillo Z_4 en el cuerpo Z_5.
21. Demostrar que el álgebra isomorfa en un cuerpo es el mismo cuerpo.
22. Mostrar que un cuerpo de fracciones del cuerpo $\mathcal{F}$ es un isomorfo para $\mathcal{F}$.
23. Demostrar que un cuerpo de fracciones del anillo $Z[\sqrt{3}]$ es un isomorfo en el cuerpo $Q(\sqrt{3})$.
24. Sean $\mathcal{K}$ y $\mathcal{K}'$ dominios de integridad isomorfos. Demostrar que los cuerpos de fracciones de esos anillos son isomorfos.

§ 6. Sistema de números reales

Cuerpos ordenados. El sistema algebraico $\langle F, < \rangle$ se denomina *conjunto totalmente ordenado* si se cumplen las condiciones siguientes:

(φ) para cualquier a, b, c de F si $a < b$ y $b < c$, se tiene entonces $a < c$;

(β) para cualquier pareja de elementos a, b de F no satisface más y nada más que a una de tres la relaciones: $a < b, a = b, b < a$.

DEFINICIÓN. Denomínese *cuerpo ordenado* al sistema algebraico $\langle F, +, -, \cdot, 1, < \rangle$ que tiene las propiedades:

(1) El álgebra $\langle F, +, -, \cdot, 1 \rangle$ es un cuerpo;

(2) El sistema $\langle F, < \rangle$ es un conjunto totalmente ordenado;

(3) Para cualquier a, b, c de F si $a < b$, entonces $a + c < b + c$ (monotonía de la adición);

(4) Para cualquier a, b, c de F si $a < b$ y $0 < c$, se tiene entonces $ac < bc$ (monotonía de la multiplicación.

El elemento a del cuerpo ordenado se llama *positivo* si $0 < a$. Por definición, $b > a$ si y solo si $a < b$. Seguido, por definición, $a \leq b$ si y solo si $a < b$ o $a = b$.

Ejemplo. Sean $\langle Q, +, -, \cdot, 1\rangle$ un cuerpo de números racionales y $<$la relación del orden banal sobre el conjunto Q. Conforme al TEOREMA 5.3, las condiciones (1) – (4) de la definición antes mencionadas se satisfacen. Por consecuencia, el sistema $\langle Q, +, -, \cdot, 1\rangle$ es un cuerpo ordenado. Este sistema se denomina *cuerpos ordenados de los números racionales.*

TEOREMA 6.1. *Sean* $\mathcal{F} = \langle F, +, -, \cdot, 1 <\rangle$ *un cuerpo ordenado y* a, b, c, d *son elementos cualquieras. Entonces se obtiene*

(1) $a < b$ *si y solo si* $\langle b - a > 0; \rangle$

(2) Para cualquier a *de* F *no satisface más y nada más que una de las tres condiciones:* $a < 0, a = 0, 0 < a$;

(3) Si $a > 0$ *y* $b > 0$, *entonces* $a + b > 0$ *y* $ab > 0$, *dicho de otro modo, el conjunto de los elementos positivos de un cuerpo ordenado es cerrado en relación a la adición y a la multiplicación;*

(4) Si $a < b$ *y* $c < d$, *se tiene entonces* $a + c < b + d$;

(5) Si $a < b$ *y* $c < 0$, *entonces* $ac > bc$;

(6) Si $a \neq 0$, *entonces* $a^2 > 0$;

(7) $1 > 0$ *y* $n \cdot 1 > 0$ *para cualquier* $n \neq 0$ *natural;*

(8) El cuerpo $\langle F, +, -, \cdot, 1\rangle$ *es un dominio de integridad.*

Demostración. (1) Conforme a la monotonía de la adición $a < b$ si y solo si $a + (-a) < b + (-a)$. Así pues, $a < b$ si y solo si $b - a > 0$.

(2) La afirmación (2) es verdadera ya que $\langle F, <\rangle$ es un conjunto totalmente ordenado (ver condición (β)).

(3) Debido a la monotonía de la adición se deduce de $a > 0$ y $b > 0$ que $a + b > b$ y $a + b > 0$. Conforme a la monotonía de la multiplicación se deduce de $a > 0$ y $b > 0$ que $ab > 0 \cdot b$ y $ab > 0$.

(4) Conforme a la monotonía de la adición si $a < b$ y $b < d$, también se obtiene $a + c < b + c$ y $b + c < b + d$. Así que, $a + c < b + d$.

(5) Conforme a (1) si $a < b$ y $c < 0$, se tiene $b - a > 0$ y $-c > 0$.

Conforme a la monotonía de la multiplicación se dedujo que $(b - a)(-c) > 0$ y $ac - bc > 0$. Así que, $ac > bc$.

(6) Conforme a la monotonía de la multiplicación si $a > 0$, se obtiene entonces $a^2 > 0$. Si, por el contrario, $-a > 0$, entonces $(-a)(-a) > 0$ y $a^2 > 0$.

(7) En el cuerpo $1 \neq 0$. Conforme a (6) $1^2 = 1 > 0$. Como el conjunto de los elementos positivos de un cuerpo ordenado se cierra en relación a la adición, se obtiene de $1 > 0$ que $n \cdot 1 > 0$ para cualquier n natural diferente de cero.

(8) Conforme al TEOREMA 5.1 para cualquier elemento a, b del cuerpo si $a \neq 0$ y $b \neq 0$. Como consecuencia, según la ley de contraposición si $ab = 0$, entonces $a = 0$ o $b = 0$. El cuerpo $\langle F, +, -, \cdot, 1\rangle$ es así un dominio de integridad. □

DEFINICIÓN. El *valor absoluto del elemento* a de un cuerpo ordenado es notado $|a|$ y es definido de la forma siguiente:

$$|a| = \begin{cases} a \ \ si \quad a \geq 0, \\ -a \ si \ \ (-a) > 0. \end{cases}$$

TEOREMA 6.2. *Sean* a *y* b *los elementos cualquieras de un cuerpo ordenado; se tiene entonces*

(1) $|a| = |-a|$;

(2) $|a| \pm a \geq 0$;

(3) $|a + b| \leq |a| + |b|$;

(4) $|ab| = |a| \cdot |b|$;

(5)$|b| \leq a \ si \ y \ solo \ si - a \leq b \leq a$.

Demostración. (1) La igualdad (1) se deduce directamente de la definición del valor absoluto del elemento.

(2) Si, $a \geq 0$, entonces se tiene $|a| = a, |a| + a \geq 0$ y $|a| - a = 0$. Si, por el contrario, $(-a) > 0$, entonces $|a| = -a, |a| - a = |a| + (-a) > 0$ y $|a| + a = 0$.
(3) Si $|a + b| = a + b$, conforme la desigualdad (2), se tiene $|a| + |b| - |a + b| = (|a| - a) + (|b| - b) \geq 0$.
Si, por el contrario, $|a + b| = -(a + b)$, del mismo modo, conforme a la desigualdad (2),
$|a| + |b| - |a + b| = (|a| + a) + (|b| + b) \geq 0$.
Así que, cualquiera que sea el caso de desigualdad (3) es verdadero.
(4) La igualdad (4) es verdadera si a o b es nulo. Si los elementos a y b son positivos, entonces $|ab| = ab = |a| \cdot |b|$. Si $a < 0$ y $b < 0$, entonces $ab = (-a)(-b) > 0$ y $|ab| = ab = (-a)(-b) = |a| \cdot |b|$. Si $a > 0$ y $b < 0$, entonces $(-ab) > 0$ y $|ab| = -ab = a \cdot (-b) = |a| \cdot |b|$. Por último, si $a < 0$ y $b > 0$, entonces $(-ab) > 0$ y $|ab| = -ab = (-a)b = |a| \cdot |b|$.
(5) La desigualdad $|b| \leq a$ se da si y solo si $(-b) \leq a$ y $b \leq a$. Así que, $|b| \leq a$ si y solo si $-a \leq b$ y $b \leq a$, es decir si $-a \leq b \leq a$. □

Sistema de números reales.

DEFINICIÓN. Un cuerpo ordenado $\mathcal{F}$ presenta un *orden arquimediano* si para cualquier elemento positivo a y b existe un número natural n tal como que se tenga $na > b$.

Sea $\langle a_0, a_1, a_2, \dots \rangle$ una sucesión infinita de elementos de un cuerpo ordenado $\mathcal{F}$. Nótese del mismo modo $\langle a_k \rangle_{k \in N}$ o $\langle a_k \rangle$.

DEFINICIÓN. El elemento a de un cuerpo ordenado $\mathcal{F}$ se denomina *límite de la sucesión* $\langle a_k \rangle$ *del elemento del cuerpo* si por cada elemento positivo ε del cuerpo hay un número natural n_0 (dependiendo de ε) tal como $|a_k - a| < \varepsilon$ para cualquier $k \geq n_0$ natural. La sucesión $\langle a_k \rangle$ que tiene un límite en el cuerpo $\mathcal{F}$ se dice *convergente* en ese cuerpo.

DEFINICIÓN. La sucesión $\langle a_k \rangle$ de los elementos de un cuerpo ordenado $\mathcal{F}$ es llamada *fundamental* (de Cauchy) sobre $\mathcal{F}$ si para cada elemento positivo ε del cuerpo existe un numero natural n_0 (dependiendo de ε) tal como que se tenga $|a_k - a_n| < \varepsilon$ para cualquier k y n naturales superiores a n_0.

DEFINICIÓN. Un cuerpo ordenado se dice *completo* si cualquier sucesión de Cauchy de los elementos de ese cuerpo converge en el anterior.

DEFINICIÓN. Denomínese *sistema de números reales* a un cuerpo completo arquimediano.

Sea $\langle R, +, -, \cdot, 1, < \rangle$ un sistema de números reales. En ese caso el álgebra $\langle R, +, -, \cdot, 1, \rangle$ es un cuerpo denominado *cuerpo de números reales.* El conjunto R se denomina *conjunto de números reales.*

Demuéstrese que dos sistemas cualquieras de números reales son isomorfos. Así que, son isomorfos los dos cuerpos de números reales.

TEOREMA 6.3. *Para dos números reales cualquieras* a *y* b *con* $b > 0$ *hay un entero* m *y un número real* r *tales como* $a = mb + r, \quad 0 \leq r < b$.

Demostración. 1°. Si $a = 0$, téngase al parecer $m = r = 0$. Plantéese que $a > 0$. El conjunto
$M = \{n \in N | (n + 1)b \leq a\}$
de los números naturales no es vacío, puesto que el sistema de números reales es arquimediano. El conjunto de números naturales está bien ordenado y M constituye un sub-conjunto no vacío del conjunto N, existe en M un mínimo elemento. Sea m el mínimo elemento de M, téngase entonces
$mb \leq a < (m + 1)b, \quad 0 \leq a - mb < b$.
Planteando $a - mb = r$, se obtiene $a = mb + r, 0 \leq r < b$.
2°. Plantéese que $a < 0$. Entonces, según la propuesta demostrada en el punto 1°, existe para los números positivos $(-a)$ y b un número real k y un número real s tal como
$-a = kb + s, \quad 0 \leq s < b$.

Como resultado, $a = (-k)b + (-s)$. Si $s = 0$, téngase la representación buscada. Si, por el contrario, $s > 0$, téngase entonces

$a = (-k-1) \cdot b + (b-s)$.

Planteando $m = -k-1$ y $r = b-s$, se obtiene

$a = mb + r,\ \ 0 \leq r < b.$ □

Sea n un número natural diferente de cero. Introdúzcase la noción de la raíz aritmética de grado n de un número natural real positivo pero previamente demuéstrese el TEOREMA siguiente.

TEOREMA 6.4. *Para cualquier número positivo a existe un único número real positivo c tal como $c^n = a$.*

Demostración. Considérese la función $f = x^n - a$ definida sobre un intervalo cerrado $[0, b]$, donde $b = a + 1$. La función f es continua sobre el intervalo y para sus terminaciones adquiridas de valores en signos diferentes, dado que $f(0) < 0 < f(b)$. Aplíquese la teoría de valores intermedios para la función f sobre el intervalo $[0, b]$. Existe según este TEOREMA un número real $c \in [0, b]$ por el cual $c^n - a = 0$, y por lo tanto,

(1) $c^n = a$.

Al parecer, $c > 0$. Supóngase que $d^n = a$ por un número positivo cualquiera d. Si además $c < d$, entonces $c^n < d^n = a$, lo cual está en contradicción con (1). Pero si $c > d, c^n > d^n = a$, lo cual también está en contradicción con (1). Así que, $d = c$. □

DEFINICIÓN. Al ser a un número real positivo y n un número natural diferente de cero. El único número real positivo c por el cual $c^n = a$ se denomina *raíz aritmética* o *raíz principal de grado n* de a y se nota por el símbolo $c^{1/n}$ o $\sqrt[n]{c}$.

Construcción de un sistema de números reales. Se denotara $\langle a_k \rangle_{k \in N}$ o $\langle a_k \rangle$ la sucesión $\langle a_0, a_1, a_2, \ldots \rangle$ de números racionales. Defínase sobre el conjunto Q^N de todas las sucesiones de los números racionales las operaciones binarias $\oplus$,$\odot$, la operación simple $\ominus$ y la operación para ningún lugar que $\overline{1}$:

$\langle a_k \rangle \ \oplus\ \langle b_k \rangle = \langle a_k + b_k \rangle$;

$\ominus\ \langle a_k \rangle = \langle -a_k \rangle$;

$\overline{1} = \langle a_k \rangle, donde\ a_k = 1$ para cualquier k natural.

Nótese $F\ (Q)$ el conjunto de todas las sucesiones de Cauchy sobre el cuerpo Q de los números naturales. Si $\langle a_k \rangle$ y $\langle b_k \rangle$ son los elementos cualquieras del conjunto $F\ (Q)$, las sucesiones $\langle a_k \rangle\ \oplus\ \langle b_k \rangle$,$\ominus\ \langle a_k \rangle$,$\langle a_k \rangle\ \odot\ \langle b_k \rangle$ pertenecen igualmente al mismo conjunto $F\ (Q)$. Así que, el conjunto $F\ (Q)$ es cerrado relativamente a las operaciones $\oplus$,$\ominus$,$\odot$.
Es fácil constatar que el álgebra $\langle F\ (Q), \oplus, \ominus, \odot, \overline{1} \rangle$ es un anillo conmutativo.

Hágase operar sobre el conjunto $F\ (Q)$ la relación binaria $\equiv$: $\langle a_k \rangle \equiv \langle b_k \rangle$ si y solo si la sucesión $\langle a_k - b_k \rangle$ converge alrededor de cero.

La relación $\equiv$ es reflexiva, transitiva y simétrica, es decir es una relación de equivalencia sobre el conjunto $F\ (Q)$. Convéngase de designar por el símbolo $[\langle a_k \rangle]$ la clase de equivalencia a la cual pertenece la sucesión $\langle a_k \rangle$. El conjunto de todas las clases de equivalencias se notan $\overline{F}, \overline{F} = F/\equiv$.

Se muestra sin duda que la relación $\equiv$ es una congruencia en el anillo $\langle F\ (Q), \oplus, \ominus, \odot,\ 1 \rangle$. Esta permite definir sobre el conjunto $\overline{F}$ las operaciones $+, -, \cdot, 1$ de la manera siguiente:

$[\langle a_k \rangle]\ +\ [\langle b_k \rangle]\ = [\langle a_k + b_k \rangle]$;

$-\ [\langle a_k \rangle] = [\langle -a_k \rangle]$;

$[\langle a_k \rangle] \cdot [\langle b_k \rangle] = [\langle a_k \cdot b_k \rangle]$;

$1 - [\overline{1}]$.

El álgebra $\langle \overline{F}, +, -, \cdot, 1 \rangle$ es el álgebra cociente del anillo $\langle F\ (Q), \oplus, \ominus, \odot,\ 1 \rangle$ que es relativo a la congruencia$\equiv$. A medida que se demuestra que el álgebra $\langle \overline{F}, +, -, \cdot, 1 \rangle$ es un cuerpo. Introdúzcase sobre el conjunto $F\ (Q)$ *la relación de orden*: para cualquier $\langle a_k \rangle\ y\ \langle b_k \rangle$ de $F\ (Q)$ se tiene $\langle a_k < b_k \rangle$,

Si existe un número natural n_0 y un número racional positivo ε tal como $b_k - a_k \geq \varepsilon$ para cualquier $k \geq n_0$.

La relación binaria $\equiv$ es una congruencia con relación a $<$, es decir que cualquier $\langle a_k \rangle$, $\langle b_k \rangle, \langle c_k \rangle$ y $\langle d_k \rangle$, de $F\ (Q)$, si $\langle a_k \rangle < \langle b_k \rangle$, $\langle a_k \rangle \equiv \langle c_k \rangle$ y $\langle b_k \rangle \equiv \langle d_k \rangle$,
Se tiene entonces $\langle c_k \rangle < \langle d_k \rangle$.

Esto permite introducir sobre el conjunto $\bar{F}$ la relación de orden: para cualquier $[\langle a_k \rangle]$ y $[\langle b_k \rangle]$ de $\bar{F}$ se plantea $[\langle a_k \rangle] < [\langle b_k \rangle]$ si $\langle a_k \rangle < \langle b_k \rangle$.

A medida que se demuestra que el sistema $\bar{\mathcal{F}} = \langle \bar{F}, +, -, \cdot, 1, < \rangle$ es un cuerpo arquimediano y toda sucesión de Cauchy sobre el cuerpo $\bar{\mathcal{F}}$ converge alrededor del elemento de ese cuerpo. El cuerpo $\bar{\mathcal{F}}$ es así un cuerpo de números reales.

Ejercicios.

1. Sean $\mathcal{F} = \langle F, +, -, \cdot, 1, < \rangle$ un cuerpo ordenado y $a, b, c, d, \in F$.

Demostrar entonces que:

(a) Si $a + c < b + c, se\ tiene\ a < b$;
(b) Si $a - b < a - c, se\ tiene\ b > c$;
(c) Si $0 < c\ y\ ac < bc, se\ tiene\ a < b$;
(d) $0 < \frac{1}{a} \leftrightarrow a > 0$;
(e) Si $0 < a < b, se\ tiene\ 0 < \frac{1}{b} < \frac{1}{a}$;
(f) Si $a < b < 0, se\ tiene\ 0 > \frac{1}{a} > \frac{1}{b}$;
(g) Si al menos uno de los números a, b, c es diferente de cero, téngase $a^2 + b^2 + c^2 > 0$.

2. Sean a, b los elementos de un cuerpo ordenado $\mathcal{F}$ y $a < b$. Demostrar que existe en $\mathcal{F}$ un elemento c tal como $a < c < b$.
3. Demostrar que la ecuación $x^2 = 2$ no tiene soluciones en un cuerpo de números racionales.
4. Demostrar que para cualquier número real positivo a la ecuación $x^2 = a$ tiene una solución en el cuerpo de los números reales.
5. Mostrar que la ecuación $x^2 + 1 = 0$ no tiene soluciones en un cuerpo de números reales.
6. Sea R^+ un conjunto de todos los números reales positivos. Demostrar que el álgebra $\langle R^+, \cdot, ^{-1} \rangle$ es un grupo el cual se denomina *grupo multiplicativo de números reales positivos*.
7. Sean a, b, c y d los números reales positivos. Demostrar que $^a/_b = {}^c/_d$ si y solo si para cualquiera de los enteros positivos m y $n\ na > mb \rightarrow nc < md$.
8. Demostrar que una aplicación idéntica es el único isomorfismo de un cuerpo de números reales en el mismo.
9. Demostrar que un sistema algebraico isomorfo o un sistema de números reales es un sistema de números reales.
10. Sea Q^N un conjunto de todas las sucesiones de números racionales. Mostrar que el álgebra $Q^N = \langle Q^N, \oplus, \ominus, \odot, \bar{1} \rangle$, donde

$\langle a_k \rangle \oplus \langle b_k \rangle = \langle a_k + b_k \rangle$;
$\ominus \langle a_k \rangle = \langle -a_k \rangle$;
$\langle a_k \rangle \odot \langle b_k \rangle = \langle a_k \cdot b_k \rangle$;
$\bar{1} = \langle a_k \rangle$, donde $a_k = 1$ para cualquier k natural, es un anillo conmutativo.

11. Sea $F(Q)$ un conjunto de todas las sucesiones de Cauchy sobre el cuerpo $Q = \langle Q, +, -, \cdot, 1 \rangle$. Mostrar que $F(Q)$ es cerrado en el anillo Q^N de todas las sucesiones de números racionales y que el álgebra $\mathcal{F}(Q) = \langle F(Q), \oplus, \ominus, \odot, \bar{1} \rangle$ es un anillo conmutativo.
12. Supóngase que $\langle a_k \rangle \equiv \langle b_k \rangle$ significa que la sucesión $\langle a_k - b_k \rangle$ converge alrededor de cero. Demostrar que:

(a) La relación $\equiv$ sobre el conjunto $F(Q)$ es una relación de equivalencia;
(b) La relación $\equiv$ es una congruencia en el anillo $\mathcal{F}(Q)$.

13. Demostrar si $\langle a_k \rangle \in f(Q)$, a k≠0 para cualquier k ∈ N y seguido de $\langle a$ k $\rangle$ no converge hacia cero, entonces se tiene

$\langle 1/a_k \rangle \in f(Q)$ y $\langle a_k \rangle \odot \langle 1/a_k \rangle = \bar{1}$

14. Demostrar que el álgebra cociente del anillo F (Q) con respecto a la congruencia $\equiv$ es una estructura.
15. Sea *F* el conjunto cociente de *F* (Q)/$\equiv$. Demostrar que el sistema

$< F,+,-,\cdot 1>$ es una estructura arquimediana.

16. Demostrar que en el sistema $< \bar{F},+,-,\cdot 1>$ toda sucesión de Cauchy de elementos del conjunto F converge en el elemento de $\bar{F}$.

§7. Cuerpo de números complejos

Extensión compleja de una estructura. Sea $\mathcal{F} =< F,+,-,\cdot ,1 >$ un cuerpo y t un elemento (un símbolo) que no pertenece a la estructura $\mathcal{F}$. La expresión de la forma $a + bt$, donde *a* y *b* son elementos cualquieras de la estructura $\mathcal{F}$, será denominada *polinomio lineal* a t sobre el cuerpo (o la forma) $\mathcal{F}$. Los elementos a y b son los *coeficientes del polinomio* $a + b$.

Dos polinomios lineales en t se denominan *iguales* si estos contienen los mismos términos (el mismo coeficiente) a los coeficientes nulos, que pueden eliminarse de la expresión (por la forma). En particular, para todos los elementos *a* y *b* del cuerpo $\mathcal{F}$

(I) $\quad a + O \cdot t = a,\ O + bt = bt.$

Desígnese para k el conjunto de todos los polinomios lineales en t en la estructura $\mathcal{F}$:

$$K = \{a + bt | a, b \in F\}$$

En el conjunto de K definimos las operaciones $+,-,\cdot$ por medio de las fórmulas siguientes:

$(II)(a + bt) + (c + dt) = (a + c) + (b + d)t$:

$(III) - (a + bt) = (-a) + (-b)t$:

$(IV)(a + bt) \cdot (c + dt) = (ac - bd) + (ad + bc)t.$

El álgebra $K =< K,+,-,\cdot ,1 >$ donde 1 es la unidad de la estructura F, se denominará álgebra de polinomios lineales.

TEOREMA 7.1. Sea $F =< F,+,-,\cdot ,1 >$ una estructura. El álgebra $K =< K,+,-,\cdot ,1 >$ de los polinomios lineales en la estructura F es un anillo conmutativo y la estructura F es su sub-anillo.

Demostración. Las operaciones principales del álgebra K constituyen prolongaciones de las operaciones principales correspondientes de la estructura F. Efectivamente, derivadas de las fórmulas $(I) - (IV)$ para cualquier a y b de F.

$$a + b = (a + 0 \cdot t) + (b + 0 \cdot t) = (a + b) + 0 \cdot t = a + b;$$

$$-a = -(a + 0 \cdot t) = (-a) + 0 \cdot t = -a;$$

$$a.\cdot b = (a + 0 \cdot t) \cdot (b + 0 \cdot t) = a.\cdot b + 0 \cdot t = a.\cdot b.$$

Además, el elemento 1 del álgebra $\mathcal{K}$ es la unidad de la estructura $\mathcal{F}$. Por lo tanto, la estructura $\mathcal{F}$ es un sub-álgebra del álgebra $\mathcal{K}$:

(1) $\mathcal{F}\ \mathcal{K}$

El álgebra $< K,+,- >$ es un grupo abeliano. De hecho, en el álgebra $\mathcal{K}$ (según la fórmula (II)) la adición es conmutativa y asociativa, dado que la adición es conmutativa y asociativa en la estructura $\mathcal{F}$. El cero de la estructura $\mathcal{F}$ es un elemento neutro con respecto a la adición en el álgebra $\mathcal{K}$, ya que en virtud de las fórmulas (I), (II), para cualquier elemento $a + bt$ de κ.

$$(a + b \cdot t) + (a + b \cdot t) + (0 + 0 \cdot t) = (a + bt)$$

Cualquier elemento $a + b \cdot t$ de K tiene su opuesto, dado que $(\ a + b \cdot t\ ) + +((-a\ ) + (-b)\ \cdot\ t) = \ 0 + 0 \cdot t = 0$. *Asi mismo* se ha establecido también que el álgebra $< K,+,- >$ es un grupo abeliano.

El álgebra $< K, \cdot, 1 >$ es un monoide conmutativo. De hecho, en el álgebra κ (según la fórmula (IV)) la multiplicación es conmutativa en virtud de la conmutatividad de la multiplicación en la estructura F. Verifíquese que en el álgebra K la multiplicación es asociativa.

$$(a+b\cdot t)\cdot[(c+dt)\cdot(e+ft)] = (a+bt)[(ce-df)+(ce-df)+(cf+de)t] =$$
$$= (ace-adf-bcf-bde)$$
$$+(acf+ade+bce-bdf)t;$$
$$[(a+bt)\cdot(c+dt)]\cdot(e+ft) = [(ac-bd)$$
$$+(ad+bc)t](e+ft)$$
$$= (ace-bdf-adf-bcf)$$
$$+(acf-bdf+ade+bce)t.$$

Entonces,

$$(a+bt)\cdot[(c+dt)\cdot(e+ft)] = [(a+bt)(c+bt)](e+ft)$$

La unidad de la estructura F es un elemento neutro con respecto a la multiplicación en álgebra K, ya que

$$(a+bt)\cdot 1 = (a+bt)(1+0\cdot t) = a+bt$$

Se estableció también que el álgebra $< K, \cdot, 1 >$ es un monoide conmutativo.

La multiplicación en el álgebra K es distributiva con respecto a la adición. Es decir,

$$[(a+bt)+(c+dt)]\cdot(e+ft) = [(a+c)+(b+d)t](e+ft) =$$
$$+(ae+ce-bf-df)+$$
$$+(af+cf+be+de)t;$$
$$(a+bt)\cdot(e+ft)+(c+dt)\cdot(e+ft) = [(ae-bf)+(af+be)t]+$$
$$+[(ce-df)+(cf+de)t] =$$
$$= (ae-bf)+(ce-df)+$$
$$+(af+be+cf+de)t.$$

Entonces,

$$[(a+bt)+(c+dt)]\cdot(e+ft) = (a+bt)\cdot(e+ft)+$$
$$+(c+dt)\cdot(e+ft)$$

En resumen, se demostró que el álgebra K es un anillo conmutativo. En virtud de (1) la estructura F es un sub-anillo del anillo K. □

DEFINICIÓN. Sea $F = < F, +, -, \cdot, 1 >$ una estructura en la cual el cuadrado de cada elemento es diferente de -1. La estructura K se denomina extensión compleja de la estructura F si se cumplen las condiciones siguientes:

(1) *F* es una sub-estructura de K;

(2) Se tiene en K un elemento u tal que $u2 = -1$;

(3) Cada elemento z de la estructura K pueda representarse por la forma de $z = a + bu$, o $a, b \in F$.

PROPOSICIÓN 7.2. *Sea F una estructura en la cual el cuadrado de cada elemento es diferente $a - 1$. Sea K la extensión compleja de la estructura F y u un elemento de la estructura K que cumple con las condiciones (2) y (3) de la definición antes mencionada. En este caso cualquier elemento z de la estructura K puede estar presente de manera única bajo la forma de $z = a + bu$,* o *$a, b \in F$*.

Demostración. Sea z un elemento cualquiera de la estructura K. Considérese dos representaciones arbitrarias de z en la forma:

(4) $z = a + bu, \quad z = c + du$

Donde $a, b, c, d \in F.\ Si\ b \neq d, entonces\ a + bu = c + du\ y\ u = \frac{c-a}{b-d}$

Entonces $u = \frac{c-a}{b-d} \in F\ y\ u^2 = -1.$ Sin embargo, es contrario a la condición según la cual el cuadrado de cada elemento de la estructura F es diferente $a\ -1$. Así que el caso donde $b \neq de$ es imposible. Por consecuencia, $b = d$ y en virtud de (4) $a = c. \square$

TEOREMA 7.3. *Sea* $F =< F, +, -, \cdot, 1 >$ *una estructura en la cual el cuadrado de cualquier elemento es diferente* $a\ -1$. *Existe entonces una extensión compleja de la estructura* F.

DEMOSTRACIÓN. Sea k el conjunto de todos los polinomios linéales en t en la estructura $\mathcal{F}$:

(1) $K = \{a + bt | a, b \in F\} \qquad (T \notin F)$

La relación de igualdad y las operaciones $+, -, \cdot$ se definen en el conjunto K por medio de las fórmulas (I)-(V). Según el TEOREMA 7.1 álgebra $\mathcal{K}$

$\mathcal{K} =< K, +, -\ \cdot, 1 >$

Es un anillo conmutativo y la estructura F constituye un sub-anillo del anillo $\mathcal{K}$:

(2) Escriba aquí la ecuación.

Demuéstrese que el anillo $\mathcal{K}$ es una estructura. En virtud de (2) el cero y la unidad de la estructura $\mathcal{F}$ son el cero y la unidad del anillo $\mathcal{K}$; así que $0_{\mathcal{K}} \neq 1_{\mathcal{K}.}$ Resta demostrar que para cualquier elemento no nulo de K se tiene en $\mathcal{K}$ un elemento el cual es opuesto. Sea $a + bt \neq 0,\ ó\ a, b \in F.$ Entonces se tiene $a \neq 0$ ó $b \neq 0.$ Como resultado, $a^2 + b^2 \neq 0$, ya que en el caso contrario $a^2 + b^2 = 0$ y $(a/b)^2 = -1$ (para b$\neq 0$) ó $(a/b)^2 = -1$, lo cual es imposible dada la hipótesis del TEOREMA. En virtud de las fórmulas (I) y (II), se tiene

$(a + bt) \cdot \left(\frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2} t\right) = 1.$

Quiere decir que el elemento $a + bt$ es invertible en $\mathcal{K}$. El anillo k es entonces una estructura.

El elemento $t\ de\ K$ cumple con la condición $t^2 = -1.$ De hecho, en virtud de las fórmulas (V) y (II), se cumple

$t \cdot t = (0 + 1 \cdot t)(1 + 1 \cdot t) = -1 + 0 \cdot t = -1$

Finalmente, en virtud de (2), la estructura F es una sub-estructura de la estructura K. Por consecuencia, estructura K es una extensión compleja de la estructura $F. \square$

TEOREMA 7.4. Sea $\mathcal{F} =< F, +, -, \cdot, 1 >$ una estructura en la cual el cuadrado de cualquier elemento es diferente a -1. Sean $\mathcal{K}$ y $\mathcal{K}'$ extensiones compleja de la estructura $\mathcal{F}$. Entonces existe un isomorfismo de la estructura $\mathcal{K}$, la cual deja invariantes en todos los elementos de la estructura $\mathcal{F}$.

Demostración. Existe en $\mathcal{K}$ un elemento u tal que bajo la forma de $a + bu$, donde $a, b \in F$. De manera análoga, existe en $\mathcal{K}'$ un elemento t tal que $t^2 = -1$ y cada elemento de estructura $\mathcal{K}'$ se representa de forma única bajo la forma de $a + bu$, donde $a, b \in F$.

Nótese ψ la función (la cual es inyectiva) de K en K' que asocia los elementos $a + bu$ de K el elemento $a + bt$ de K'. Por otra parte ψ respeta las operaciones principales de la estructura $\mathcal{K}$. De hecho, ya que

$(a + bu) + (c + du) = (a + c) + (b + d)u,$

$-(a + bu) = (-a) + (-b)u,$

$(a + bu)(c + du) = (ac - db) + (ad + bc)\ u,$

Se tiene

$\psi\big((a + bu) + (c + du)\big) = (a + c) + (b + d)t = (a + bt) +$

$+(c + dt) = \psi(a + bu) + \psi(c + du),$

$\psi\big(-(a + bu)\big) = (-a) + (-b) += -(a + bt) =$

$$= -\psi(a + bu),$$

$$\psi\big((a + bu)(c + du)\big) = (ac - bd) + (ad + bc)t =$$

$$= (a + bt) \cdot (c + dt) = \psi(a + bu) \cdot \psi(c + du).$$

Además, $\psi(1) = 1$ y $\psi(a) = a$ para cualquier a elemento de la estructura $\mathcal{F}$. Así mismo, ψ es una función isomorfa de la estructura K en la estructura K', que deja invariante todos los elementos de la estructura $\mathcal{F}$. Así mismo, ψ es una función isomorfa de la estructura $\mathcal{K}$ en la estructura $\mathcal{K}'$ la cual deja invariantes todos los elementos de la estructura $\mathcal{F}$. □

Estructura de números complejos. En una estructura ordenada el cuadrado de cualquier elemento nulo es positivo. Así bien, en una estructura de números reales el cuadrado de cualquier número real es diferente a -1. En virtud del TEOREMA 7.3 existe una extensión compleja de a la estructura de números reales $\mathcal{R}$. Según el TEOREMA 7.4 cada dos extensiones complejas de la estructura $\mathcal{R}$ de números reales son isomorfas.

DEFINICIÓN. Se denomina estructura de números complejos una extensión compleja de la estructura de números reales.

Sea $\mathcal{R} =< R, +, -, \cdot, 1 >$ una estructura de números reales. Sea $\mathcal{C}$ una estructura de números complejos, extensión compleja de la estructura $\mathcal{R}$. El conjunto de la base de la estructura $\mathcal{C}$ se denota c. Los elementos del conjunto C se denominan números complejos. Desígnese para i un número complejo por el cual $i^2 = -1$, de manera que cualquier número complejo z de C puede representarse bajo la forma de $\mathcal{Z} = a + bi$, donde $a, b \in R$. Esta representación se denomina forma algebraica de números z. El número i se denomina unidad imaginaria de los números complejos.

TEOREMA 7.5. Sean $\mathbb{C} =< C, +, -, \cdot, 1 >$ una estructura de números complejos, extensión compleja de la estructura R de números reales arbitrarios.

Entonces, se obtiene

(1) $a + bi = c + di$ si y solo si $a = c \; y \; b = d$;

(2) $(a + bi) + (c + di) = (a + c) + (b + d)i$:

(3) $-(a + bi) = (-a) + (-b)i$;

(4) $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$;

(5) $si\ a + bi \neq 0, entonces\ (a + b)^{-1} = \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2} \cdot i.$

Demostración. Sea $a + bi = c + di$. Si $b = d$, se obtiene $a = c$, pero si $b \neq d$ se deduce que $i = \frac{c-a}{b-d} \in R \; y \; \left(\frac{c-a}{b-d}\right)^2 = -1$, lo cual es imposible. Así mismo, el caso de $b \neq d$ es inaceptable. $\mathcal{C}$ que son una estructura, se tiene las igualdades (2) (3) y (4).

Sea $a + bi \neq 0$. En virtud de (1) $a \neq 0$ ó $b \neq 0 \; y \; a - bi \neq 0$. Dado que, el producto de dos elementos cualesquiera no nulos de la estructura $\mathcal{C}$ es diferente a cero, se tiene$(a + bi) = a^2 + b^2 = 0$. Como resultado se tiene

$(a + bi)^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{(\cdot b)}{a^2+b^2} i.$ □

DEFINICIÓN. Se denomina estructura numérica a toda subestructura de la estructura de números complejos.

Toda estructura numérica tiene una subestructura de números racionales. De hecho, sea $F =< F, +, -, \cdot, 1 >$ una estructura numérica cualquiera. Dado que $0,1 \in F$ y el conjunto F es cerrado relativamente a la operación $+, -$ se deduce que $n = 1 + \cdots + 1 \in F \; y - n \in F$. Así que, F contiene todo los números enteros. El conjunto F es cerrado con relación a la división y, por sucesión, conserva todos los elementos de la forma mn^{-1} escrito m/n. Así que, F encierra el conjunto Q de todos los números racionales. El conjunto Q es cerrado relativamente a las operaciones principales de la estructura F y cualquier elemento no nulo de Q es invertible en Q. Se deduce que, el álgebra $Q, Q =< Q, +, -, \cdot, 1 >$, es una

subestructura de la estructura F. Como resultado la estructura numérica F contiene una subestructura Q de números racionales.

DEFINICIÓN. Se denomina anillo numérico a cualquier sub-anillos de una estructura de números complejos.

Así que, por ejemplo, los anillos Z, Q, C son numéricos.

El sub-anillo de la estructura C generada para el elemento i y se escribe $Z[i]$ es una estructura numérica.

Números conjugados. Si $z = a + b$, donde $a, b \in \boldsymbol{R}$, entonces el número $a - bi$ se escriben $\bar{z}$.

DEFINICIÓN. Los números complejos $z = a + bi \; y \; \bar{z} = a + bi$ se denominan conjugados.

Recuérdese que la ecuación isomorfa de una estructura sobre ella misma se denomina automorfismo de la estructura.

TEOREMA 7.6. Si $z \; y \; z'$ son números complejos cualesquiera, entonces se tiene

(1) $\overline{z+z'} = \bar{z} + z'$;
(2) $\overline{(-z)} = -\bar{z}$;
(3) $\overline{z \cdot z'} = \bar{z} \cdot z'$;
(4) $\overline{(\bar{z})} = z$;
(5) $z = \bar{z} \; si \; y \; solo \; si \; z \in \boldsymbol{R}$;
(6) Si $z = a + bi, entonces \; z \cdot \bar{z} = a^2 + b^2$.

La demostración del TEOREMA queda a opción del lector.

COROLARIOS 7.7 La ecuación de una estructura de números complejos $\mathcal{C}$ en ella misma, la cual hace corresponder a cualquier número complejo z su conjugado
$\bar{z}$ es un automorfismo de la estructura $\mathcal{C}$, la cual deja invariantes los números reales.

Módulo de un número complejo. Se introduce la noción de módulo de un número complejo.

DEFINICIÓN. Se denomina módulo de un número complejo a $a + bi < a, b \in \boldsymbol{R} >$ la raíz cuadrada aritmética del número $(a^2 + b^2)^{1/2}$. El módulo de un número complejo $z = a + bi$, se escribe $|z|$ó$|a + bi|$. Así mismo, por la definición. $|z|^2 = a^2 + b^2$.

TEOREMA 7.8 Para cualquier número complejo $z \; y \; u$, se tiene

(1) $|z|^2 = z \cdot \bar{z}$;
(2) $|z| = 0 \; si \quad y \; solo \; si \;\; z = 0$;
(3) $|zu| = |z| \cdot |u|$;
(4) $|z^{-1}| = |z|^{-1} \; para \; z \neq 0$;
(5) $|z + u| \leq |z| + |u|$;
(6) $|z| - |u| \leq |z + u|$;
(7) $\big||z| - |u|\big| \leq |z + u|$.

DEMOSTRACIÓN. (1) Si $z = a + bi, \; \bar{z} = a - bi \; y \; z \cdot \bar{z} = a^2 + b^2 = |z|^2$.

(2)Si $|z|=|a + bi| = 0, entonces \; |z|^2 = a^2 + b^2 = 0$. sin embargo, como $a \; y \; b$ son números reales, se deduce $a^2 + b^2 = 0 \; que \; a = b = 0, es \; decir \; que \; z = 0$

(3) en virtud de (1)

$$|zu|^2 = (zu)\overline{(zu)} = (z\bar{z})(u\bar{u}) = |z|^2|u|^2$$
$$= (|z| \cdot |u|)^{2.}$$

De igualdad $|zu|^2 = (|z| \cdot |u|)^2$se deduce a fórmula (3).

(4) según (3), para $z \neq 0$

$$|z \cdot z^{-1}| = |z| \cdot |z^{-1}| = 1.$$

Por consiguiente $|z^{-1}| = |z|^{-1}$.

(5) de (1) se cumple

$$|z+1|^2 = (zj+1)\cdot(\bar{z}+1) = |z|^2 + z + \bar{z} + 1.$$

Además, si $z = a + bi$, $z + \bar{z} = 2a \leq 2a(a^2+b^2)^{1/2} = 2|z|$. Así mismo, $|z+u|^2 = \leq (|z|+1)^2$; como resultado, $|z+1| \leq |z|+1$. Apoyándose de la fórmula (3) y de la última desigualdad, se concluye que para $u \neq 0$

$$|z+u| = |u(zu^{-1}+1)| = |u||zu^{-1}+1 \leq|$$

$$\leq |u|(|zu^{-1}|+1) = |u|(|z||u|^{-1}+1.)$$

Entonces, $|z+u| \leq |z| + |u|$.

(6)dado que $z = -u + (z+u)y\ |-4| = |u|, en\ virtud\ de\ (5)|z| \leq |-u| + |z+u| = |u| + |z+u|. Entonces\ |z| - |u| \leq |z+u|$.

Interpretación geométrica de números complejos. A cada número complejo $z = a + bi$ hagamos corresponder un punto $M(a,b)$ del plano (con sistemas de coordenadas rectangulares) de abscisa a y ordenado b. El punto $M(a,b)$se denomina afijo de $a + bi$.

Para cada dos números complejos $a + bi$ y $c + di$ la igualdad $a + bi = c + di$ sólo tiene lugar si y sólo si $a = c$ y $b = d$. También la ecuación que asocia a cada número complejo $a + bi$ el punto $M(a,b)$ del plano de coordenadas constituye una ecuación inyectiva del conjunto C de los números complejos sobre el conjunto de los puntos del plano de coordenadas. El plano de coordenadas cuyos puntos son la representación geométrica de los números complejos se llama plano complejo.

Sean r y φ coordenadas polares del punto $M(0\ es\ el\ origen, 0x\ el\ eje\ polar)$. Entonces $r = (a^2 + b^2)^{1/2}, dicho\ de\ otra\ manera, r$ es el módulo del número complejo $a + bi$.

Los números reales se representan por los puntos del eje de abscisas; es justamente por eso que se llama eje real al eje de abscisas. Los puntos del eje de ordenadas representan los *números puramente imaginarios*, es decir, los números de la forma bi, donde $b \in R$, también el eje de ordenadas se llama *eje imaginario*.

Los *números conjugados* $z\ y\ \bar{z}$ se figuran por los puntos simétricos en relación al eje real. Los *números* z y $-z$ *mutuamente opuestos* se representan por los puntos simétricos en relación al origen de coordenadas.

Los afijos de números complejos del mismo módulo $r, r > 0$, se disponen sobre un circuito de raya r y que tiene por centro el origen de las coordenadas.

Represéntese sobre un plano complejo los números complejos $z_1 = a_1 + b_1, i, z_2 = a_2 + b_2 i$, así mismo su suma $z_3 = (a_2 + a_2) + (b_2 + b_2)i$ para los puntos $M_1, M_2\ y\ M_3$ respectivamente. El segmento geométricamente orientado OM_3 se obtiene a partir de segmentos orientados OM_1 y OM_2 que cumplen la regla de paralelogramo.

Ejercicios.

1. Buscar sobre el plano los afijos de los números complejos $1, i, 1+i, 1-i, -1-i, 1+i\sqrt{3},\ \sqrt{3}-i$.
2. Sean dados un número real positivo a y un número complejo c. Buscar el conjunto de puntos del plano que constituyen los afijos de números complejos z y que cumplen con las condiciones:

   (a) $|z| = a$; (b) $|z-c| = a$;

   (c)$|z| < a$; $(d)|z-c| < a$;

   (e)$|z-1| \leq 1$; (f) $|z-1-i| < \sqrt{2}$;

   (g) $|z-1| + |z+1| = 2$

3. Resolver las ecuaciones.

(a) $(1-i)\bar{z}-3iz=2-i$;

(b) z· $\bar{z}-2\bar{z}=3-i$;

(c) $z\cdot\bar{z}+3(z-\bar{z})=4+3i$

(d) $z\cdot\bar{z}+3(z+\bar{z})=7$;

(e) $z\cdot\bar{z}+3(z+\bar{z})=3$.

4. Demostrar que para cualquier número complejo $z_1\ y\ z_2$ se tiene la igualdad $|z_1+z_2|^2+|z_1+z_2|^2=2(|z_1|^2+|z_2|^2)$. ¿Cuál es la interpretación geométrica de esta igualdad?

5. Resolver el sistema de ecuaciones.

(a) $ix+(1+i)y=3-i$; $\quad(1-i)x-(6-i)\ y=4$;

(b) $(2+i)x-(3+i)\ y=i$; $\quad(3-i)\bar{x}+(2+i)\bar{y}=-i$.

6. Resolver las ecuaciones (en una estructura de números complejos):

(a) $z^2+(4+3i)z+1+5i=0$;

(b) $z^2+5z+9=0$;

(c) $z^2+z+1+i=0$;

(d) $z^2+1=0$;

(e) $z^2+1;0$.

7. Demostrar que en una estructura de números complejos sólo existe un único automorfismo diferente del automorfismo idéntico que transforma de nuevo los números reales en números reales.

8. Demostrar que cada anillo numérico contiene un sub-anillo de enteros.

9. Sea C_1 un conjunto de todas las matrices cuadradas de orden dos del aspecto $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ en a y b reales. Demostrar que el álgebra $\langle C_1,+,-,\cdot,e\rangle$ del tipo $(2,1,2,0)$, donde $+,-,\cdot$ son operaciones banales en las matrices y $e=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ es una estructura isomorfa en la estructura de números complejos.

10. Sea K un conjunto de números complejos de la forma $m+ni$ en m y n enteros. Demostrar que el álgebra $\langle K,+,-,\cdot,1\rangle$ es un dominio de integridad (un anillo de integridad). Este anillo se llama *anillo de enteros de Gauss.*

11. Describir una sub-estructura de una estructura de números complejos generados por el número i y números racionales.

§ 8.Forma trigonométrica de un número complejo.

Extracción de raíces a partir de números complejos

Forma trigonométrica de un número complejo. A la par de la forma algebraica del número complejo se utiliza frecuentemente la forma trigonométrica.

PROPOSICIÓN 8.1. *Para todo número real x y $\mathcal{Y}$ que cumple con la condición*

1) $x^2+y^2=1$,

Existe un número real único φ, tal que

(2)$x=\cos\varphi, y=\sin\varphi, \quad 0\le\psi<2\pi.$

Demostración. Supongamos que los números reales cumplen la condición (1), entonces

(3) $|x|\le 1.$

Cualquier número real que cumple con la condición (3) pertenece al dominio de valores de la función cos del intervalo cerrado $[0,\pi]$ existe entonces un número real φ tal como

(4) $x=\cos\varphi, \qquad 0\le\varphi\le\pi.$

En virtud de (1) y (4) $y^2 = sin^2\,\varphi\; e\; y = \pm\sin\varphi$. Si $y = \sin\varphi$, plantéese $\varphi = \psi$. Pero si $y = -\sin\psi$, plantéese $\varphi = 2\pi - \psi$. En cualquier caso el número real φ cumple con las condiciones (2).

Supóngase que θ es un número real cualquiera que cumple con las condiciones

(5) $x = \sin\theta, \quad y = \sin\theta, \quad 0 \le \theta < 2\pi.$

Admítase que $\theta \le \varphi$, entonces

$\sin(\varphi - \theta) = \sin\varphi\ \cos\theta - \cos\varphi\,\sin\theta = yx - xy = 0.$

Sin embargo $0 \le \varphi - \theta 2\pi$, también la igualdad $\sin(\varphi - \theta) = 0$ solo tiene lugar para $\varphi - \theta = 0$ ó $\varphi - \theta = \pi$. Si $\varphi - \theta = \pi, \cos\varphi = -\cos\theta = -x = -\cos\varphi,\ \sin\varphi = -\sin\theta = -y = -\sin\varphi$; a partir de las igualdades $\cos\varphi = -\cos\varphi, \sin\varphi = -\sin\varphi$ se deduce que $\cos\varphi = \sin\varphi = 0$, lo cual es imposible. Entonces, el caso donde $\varphi - \theta = \pi$ es imposible. Como resultado, $\varphi - \theta = 0\; y\; \varphi = \theta$. □

TEOREMA 8.2. *Para cualquier número complejo z diferente de cero existe un único par de números reales r* y ψ tal como

(1) $z = r(\cos\varphi + i\sin\varphi), \quad 0 < r, \quad 0 \le \varphi < 2\pi.$

Demostración. Si r cumple las condiciones (1), entonces se tiene $|z|^2 = r^2(cos^2\varphi + sin^2\varphi) = r^2$ y $r = |z|$. No hay más de un número real r que cumpla con las condiciones (1).

Sea $z = a + bi \ne 0$, donde a, b son números reales. Plantéese $r = (a^2 + b^2)^{1/2}, r > 0$. Entonces $(a/r)^2 + (b/r)^2 = 1$. En virtud de la proposición 8.1 existe un número real único φ que cumple con las condiciones

(2) $a/r = \cos\varphi, \quad b/r = \sin\varphi, \quad 0 \le \varphi < 2\pi.$

Como $r > 0\; y\; z = r\left(\frac{a}{r} + \frac{b}{r}i\right)$, se deduce de (2)

(3) $z = r(cos\varphi + i\,sin\,\varphi), \quad 0 \le \varphi < 2\pi.$

Por otra parte, de (3) se deducen las igualdades $a + bi = r\cos\varphi + r\sin\varphi \cdot i,\ a = r\cos\varphi,\ b = r\sin\varphi$. Así que la condición (2) se deriva de la condición (3). Por consiguiente, las condiciones (2) y (3) son equipolentes para $r > 0$. Solo existe un único par de números reales que cumplen con las condiciones (1). □

DEFINICIÓN. Se denomina *forma trigonométrica del número complejo z* su representación $z = r(\cos\varphi + i\sin\varphi)$, donde r y φ son números reales y $r \ge 0$.

TEOREMA 8.3 *Sean*

(1) $z = r(\cos\varphi + i\sin\varphi), \quad r > 0,$

(2) $z = r_1(\cos\psi + \cos\psi), \quad r_1 > 0,$

Dos representaciones del número complejo z bajo la forma trigonométrica. Entonces se tiene $r = r_1 = |z|$ *y hay un entero k tal como $\varphi - \psi = 2\pi k$.*

Demostración. Se estableció en el TEOREMA 8.2 que de (1) y (2) se deducen respectivamente las igualdades $r = |z|$ y $r_1 = |z|$ ó $r = r_1 = |z|$. Según el TEOREMA 6.3 existe para el par de números φ y 2π un número real α y un entero m tales como

(3) $\varphi = 2\pi m + \propto, \quad 0 \le \beta < 2\pi.$

De manera análoga, para los números ψ y 2π existe un número real β y un entero n tales como

(4) $\psi 2\pi n + \beta, \quad 0 \le \beta < 2\pi.$

En la base de las fórmulas (1), (3), se obtiene que $r = |z|$ y

(5) $z = |z|(\cos\propto + i\sin\propto).$

En virtud de las fórmulas (2), (4), se llega a $r_1 = |z|$ y a

(6) $z = |z|(\cos\beta + i\ sen\ \beta)$.

Ya que $|z| \neq 0$, a partir de (5) y (6) se obtiene

(7) $\cos \propto + i\ sen\ \propto = cos\beta + i\ sen\beta$.

Como $0 \leq \propto, \beta < 2\pi$, según el TEOREMA 8.2, se obtiene de (7)

(8) $\propto = \beta$

Sobre la base de (3), (4) y (8) se concluye que $\varphi - \psi = 2\pi k$, donde $k = m - n$. □

TEOREMA 8.4. *Sean* $z = |z|(cos\ \varphi + i\ sen\ \varphi), z_1 = |z_1| \times (cos\psi + i\ sen\psi)$, donde $\varphi\ y\ \psi$ son números reales, entonces

(1) $Zz_1 = |z||z_1|[\cos(\varphi + \psi) + i\ sen(\varphi + \psi)]$

(2) $\frac{z}{z_1} = \frac{z}{|z_1|}[\cos(\varphi - \psi) + i\ sen\ (\varphi - \psi)]$ para $z_1 \neq 0$;

(3) $z^n = |z|^n(\cos n\varphi + i\ sen\ n\varphi)$ para cualquier n natural;

(4) $(cos\varphi + i\ sen\ \varphi)^n = \cos n\varphi + i\ sen\ n\varphi$.

Demostración. En virtud de la distributividad de la multiplicación de números complejos en relación a la adición, se obtiene

$$z \cdot z_1 = |z| \cdot |z_1|[(cos\varphi\ cos\psi - sen\varphi sen\psi) +] \\ +(cos\varphi sen\psi + cos\psi sen\varphi)i.$$

De donde se deduce la formula (1), ya que

$cos\varphi\ cos\psi - sen\varphi\ sen\psi = \cos(\varphi + \psi)$;

$cos\varphi\ sen\psi + cos\psi\ sen\varphi = sen(\varphi + \psi)$.

En virtud de la formula (1), se obtiene

$$(cos\psi + i\ sen\psi)\big(\cos(-\psi) + i\ sen\ (-\psi)\big) = \\ = \cos 0 + i\ sen\ 0 = 1,$$

Y, por consiguiente

$\frac{1}{cos\psi + i\ sen\psi} = \cos(-\psi) + i\ sen(-\psi)$,

Y para $z_1 \neq 0$

$\frac{1}{z_1} = \frac{1}{|z_1|}\big(\cos(-\psi) + i\ sen\ (-\psi)\big)$.

Como resultado, según la formula (1)

$\frac{z}{z_1} = z \cdot \frac{1}{z_1} = \frac{|1|}{|z_1|} \cdot [\cos(\varphi - \psi) + i\ sen(\varphi - \psi)]$.

La fórmula (3) se demuestra por recurrencia en n que se inspira de la fórmula (1). La fórmula (4) se obtiene a partir de la fórmula (3) para $|z| = 1$. □

Las fórmulas (3) y (4) se llaman *fórmulas de Moivre*.

Raíces n-ésima de la unidad. Sea n cualquier número natural diferente a cero.

DEFINICIÓN. Un número complejo w que cumple con la condición $w^n = 1$ se llama *raíz* $n - ésima$ *de la unidad.*

TEOREMA 8.5. *Existe exactamente n diferentes raíces n-ésima de la unidad que se obtienen algunas por la fórmula*

$w_k = cos\frac{2\pi k}{n} + i\ sen\ \frac{2\pi k}{n}\ con\ k = 0,1, \dots, n1.$

Demostración. Cada uno de los números w_k constituye una raíz n-ésima de la unidad, ya que, según la fórmula de Moivre,

$$w_k^n = (cos\frac{2\pi k}{n} + i\ sen\frac{2\pi k}{n})^n = cos2\pi k + i\ sen2\pi k = 1.$$

Los números reales $\frac{2\pi\cdot 0}{n}, \frac{2\pi\cdot 1,}{n}, \dots, \frac{2\pi(n-1)}{n}$ no son negativos, inferiores al número 2π y difieren dos por dos. Entonces, según el TEOREMA 8.2, los números complejos $w_0, w_1, \dots w_{n-1}$ difieren dos por dos.

Nos queda demostrar que una raíz n-ésima cualquiera de la unidad pertenece al conjunto $\{w_0, w_1, \dots, w_{n-1}\}$. Según el TEOREMA 8.2 el número w se puede figurar bajo la forma $w = |w|(cos\varphi + i\ sen\ \varphi)$, el número real φ que cumple con las condiciones

(1) $0 \le \varphi < 2\pi$.

Como $w^n = 1, |w|^n = 1$ y, según el TEOREMA 6.4, $|w| = 1$. Como resultado, $w = cos\varphi + i\ sen\varphi$. Según la fórmula de Moivre $w^n = cos\varphi + i\ sen\varphi$. También la igualdad $w^n = 1$ puede escribirse bajo la forma

(2) $\cos n\varphi + i\ sen\ n\varphi = \cos 0 + i\ sen\ 0$.

Según el TEOREMA 8.3, se deduce de (2) que $n\varphi - 0 = 2\pi k$ para un entero k, por consiguiente, $\varphi = \frac{2\pi k}{n}$. Por otra parte, en virtud de (1), $0 \le \varphi = \frac{2\pi k}{n} < 2\pi$ y, por consiguiente, $0 \le k < n$. Entonces

$w = cos\frac{2\pi k}{n} + i\ sen\ \frac{2\pi k}{n} = w_k \in \{w_0, w_1, \dots, w_{n-1}\}$. □

COROLARIO 8.6. *Los puntos del plano complejo que representa las raíces n-ésima de la unidad ocupan las cimas de un polígono regular en n ángulos inscrito en el círculo de la línea unidad y del centro en el origen de coordenadas, además, una de las cimas se encuentra en el punto* (0,1).

DEFINICIÓN. El número complejo w se denomina *raíz primitiva n-ésima de la unidad* $(n \ge 1)$ si el conjunto de números $\{w^0, w^1, \dots, w^{n-1}\}$ constituye un conjunto de todas las soluciones de las ecuaciones $z^n = 1$.

Es así, por ejemplo, que para cualquier $n \ge 1$ natural el número $w_1 = cos\frac{2\pi}{n} + i\ sen\ \frac{2\pi}{n}$ es, en virtud del TEOREMA 8.5, la raíz primitiva $n - ésima$ de la unidad.

Raíces n-ésima de un número complejo arbitrario. La forma trigonométrica de un número complejo resuelve totalmente el problema de la extracción de las raíces de número complejo.

TEOREMA. 8.7. *Sean* $c = |c|(\cos\varphi + i\ sen\ \varphi)$ *un número complejo diferente a cero y* n *un número natural no nulo. Hay* n *raíces n- ésima distinto del número c y, todos, se obtienen con la ayuda de la fórmula*

$$u_k = |c|^{1/n}(\cos\frac{\varphi + 2\pi k}{n} + i\ sen\ \frac{\varphi + 2\pi k)}{n},\quad k = 0, 1 \dots., n-1$$

Demostración. Muéstrese que se obtiene

(1) $u_k = u_0 w_k, \qquad k = 0,1, \dots., n-1$

Donde $w_0, \dots, w_{n-1}$ son las raíces n-ésimas de la unidad y

$u_0 = |c|^{1/n}\left(cos\frac{\varphi}{n} + i\ sen\frac{\varphi}{n}\right)$.

En efecto, en virtud de la fórmula de Moivre

$u_k = |c|^{1/n}\left(cos\frac{\varphi}{n} + i\ sen\ \frac{\varphi}{n}\right)\left(cos\frac{2\pi k}{n} + i\ sen\ \frac{2\pi k}{n}\right) = u_0 w_k$.

Cada uno de los números u_k es una raíz n-ésima del número c, ya que, en virtud de (1)

$u_k^n = u_0^n w_k^n = u_0^n = \left(|c|^{1/n}\right)^n(\cos\frac{\varphi}{n} + i\ sen\ \frac{\varphi}{n})^n =$

$= |c|(\cos\varphi + i\ sen\ \varphi = c$.

Si u es una raíz n-ésima arbitraria del número c, entonces $(uu_0^{-1})^n = u^n(u_0^n)^{-1} = cc^{-1} = 1$. Así,

$uu_0^{-1} \in \{w_0, \dots, w_{n-1}\}$

Y en virtud de (1)

$u \in \{u_0 w_0, \dots, u_0 w_{n-1}\} = \{u_0, \dots, u_{n-1}\}$.

Como resultado, el conjunto $\{u_0, \dots, u_{n-1}\}$ es el conjunto de todas las raíces n-ésimas del número c. este conjunto contiene exactamente n elementos distintos, dado que

$\{u_0, \dots, u_{n-1}\} = \{u_0 w_0, \dots, u_0 w_{n-1}\}$,

$u_0 \neq 0$ y los números $w_0, \dots, w_{n-1}$ difieren dos por dos según el TEOREMA 8.2). □

Ejercicios

1. Representar en forma trigonométrica los números complejos.

$1, i, -1-i, 1+i, 1-i, -\frac{1}{2} + i\frac{\sqrt{\bar{3}}}{2}, \sqrt{\bar{3}} + i.$

2. Buscar el conjunto de los puntos del plano que representa los números complejos z para los cuales:

(a) $\arg z = 0$, $(b) \arg z = \frac{\pi}{3}$; $(c) \arg z = \pi$; $(d) \arg z = \frac{\pi}{2}$.

3. ¿En qué condiciones el módulo de la suma de dos números complejos es igual a la suma de módulos de términos?
4. ¿En qué condiciones el módulo de la suma de dos números complejos es igual a la diferencia de módulos de términos?
5. Describir las aplicaciones siguientes (**C**→ $\boldsymbol{C}$)**:**

(a) $z \mapsto \bar{z}$; $(b) z \mapsto \frac{1}{z} (z \neq 0)$; $(c) z \mapsto -i\bar{z}$;

(d) $z \mapsto i\bar{z}$; $(e) z \mapsto rz$, donde r es un número positivo;

(f) $z \mapsto (\cos\varphi + i\, sen\, \varphi)$; $(g) z \mapsto -\bar{z}$;

(h) $z \mapsto r(\cos\varphi + i\, sen\, \varphi)$; $(i)\ z \mapsto \bar{z}^{-1}$.

6. Sea $w = cos\frac{2\pi}{3} + i\, sen\, \frac{2\pi}{3}$ y n un número natural. Calcular:

(a) $(1+w)^n$; $(b) w^n + \bar{w}^n$.

7. Calcular la suma $\frac{1}{2} + cosx + cos2x + \cdots + cosnx$.

8. Demostrar que $senx + sen2x + \cdots + sen\, nx = \frac{sen\frac{n+1}{2}x \cdot sen\frac{nx}{2}}{sen\frac{x}{2}}$.

9. Expresar con la ayuda del $cos\ x$ y $sen\ x$:

(a) $\cos 5x$; $(b) sen5x$; $(c) \cos 6x$; $(d)\ sen\ 6x$; $(e) \cos 8x$.

10. Buscar las fórmulas que expresan $cos\ nx$ y $sen\ nx$ con la ayuda $cos\ x$ y $sen\ x$.

11. Expresar en forma de polinomio trigonométrico de primer grado de coseno y de seno de los ángulos múltiples de x:

(a) $sen^3 x$; $(b) cos^5 x$; $(c) sen^5 x$; $(d)\ cos^6 x$

12. Encontrar todas las raíces de la unidad de índice:

(a) 2; (b) 3; (c) 6; (d) 8; (e) 12; (f) 24.

13. Encontrar todas las raíces complejas de las ecuaciones:

(a) $z^3 + i = 0$; $(b) z^3 + 2 + 2i = 0$; $(c) z^4 + \frac{4}{2} + i\frac{\sqrt{3}}{2} = 0$;

(d) $z^6 + i = 0$; $(e) z^5 - 1 = 0$.

14. Encontrar la suma y el producto de todas las raíces n-ésimas de 1.

15. Sea $\varepsilon = \cos\frac{2\pi}{n} + i\, sen\frac{2\pi}{n}$, donde n es un entero positivo. Demostrar que el número complejo z es una raíz primitiva n-ésima de la unidad si y solo si $z = \varepsilon^m$ para un número natural m primero con n.

16. Buscar las raíces primitivas de índice:

(a) 2; (b) 3; (c) 4; (d) 5; (e) 6; (f) 8; (g) 12; (h) 24.

17. Buscar todos los números complejos que cumplen con la condición $\bar{z} = z^{n-1}$, y $\bar{z}$ donde n es un entero positivo el conjugado de z.

18. Demostrar las afirmaciones siguientes:

(a) el producto de la raíz m-ésima de 1 para la raíz n-esima de 1 es una raíz mn-ésima de 1;

(b) si m y n están primeros entre ellos, hay un solo número complejo z que cumple con las condiciones $z^m = 1\ y\ z^n = 1$;

(c) si los números m y n están primeros entre ellos, todas las raíces mn-ésimas de 1 se obtienen entonces por la multiplicación de raíces m-ésimas de 1 para las raíces n-ésimas de 1.

(d) si m y n están primeros entre ellos, el producto del raíz primitiva m-ésima de 1 para la raíz primitiva n-ésima de 1 es entonces una raíz primitiva mn-ésima de 1 y recíprocamente.

CAPITULO V
ESPACIOS VECTORIALES ARITMETICOS Y SISTEMASDE ECUACIONES LINEALES

§ 1. Espacios vectoriales aritméticos

Espacio vectorial aritmético en n dimensiones. Sean $\mathcal{F}$ una estructura de la elección arbitraria, $\mathcal{F} = < \mathrm{F}, +, -, \cdot, 1 >$, y F su conjunto de base. Los elementos del conjunto F se denominan escalares, F el conjunto de los escalares y $\mathcal{F}$ la estructura de escalares. Sea n un número natural fijo a parte de cero.

DEFINICIÓN. *Se denomina vector en n dimensiones en la estructura $\mathcal{F}$* a cualquier

Sucesión de n elementos de la estructura $\mathcal{F}$. El conjunto de todos los vectores en n dimensiones sobre la estructura $\mathcal{F}$ se escribe F^n.

Generalmente el vector se presenta bajo forma de una línea o una columna. En este párrafo se escribirá el vector en n dimensiones en línea.

$(\alpha_1, \alpha_2, \dots, \alpha_n)$

Donde $\alpha 1, \alpha 2, \dots, \alpha_n \epsilon F$.

Introduzcamos en el conjunto de vectores en n dimensiones sobre la estructura $\mathcal{F}$ la relación de igualdad, la operación de adición de vectores y la operación de multiplicación del vector por un escalar.

DEFINICIÓN. Los vectores $(\alpha_1, \dots, \alpha_n)\ y\ (\beta_1, \dots, \beta_n)\ se\ llaman\ iguales\ si\ \alpha_1 = \beta_1, \dots, \alpha_n = \beta_n.$

DEFINICIÓN. Se denomina *suma de vectores* $(\alpha_1, \dots, \alpha_n)$ y $(\beta_1, \dots, \beta_n)$ el vector $(\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$, es decir $(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$.

DEFINICIÓN. Se denomina *producto de un escalar λ para el vector* $(\alpha_1, \dots, \alpha_n)$ el vector $(\lambda\alpha_1, \dots, \alpha_n)$, es decir, $\lambda(\alpha_1, \dots, \alpha_n) = (\lambda\alpha_1, \dots, \alpha_n)$.

La operación de multiplicación por un escalar λ se designará por el símbolo ω_λ, es decir $\omega_\lambda(\alpha_1, \dots, \alpha_n) = \lambda(\alpha_1, \dots, \alpha_n)$.

Para cada λ de F ω_λ es una operación simple sobre el conjunto F^n de vectores en n dimensiones.

El vector $(0, \dots, 0)$ se denomina *vector nulo* y se denota 0. Un vector nulo es un elemento neutro en relación a la adición.

El vector $(-1) \cdot (\alpha_1, \dots, \alpha_n)$ se denomina *vector opuesto del vector* $a = (\alpha_1, \dots, \alpha_n)$ y se escribe $-\mathbb{a}$. naturalmente $a + (-a) = 0$.

DEFINICIÓN**.** Se denomina *espacio vectorial aritmética a n dimensiones en la estructura $\mathcal{F}$* el conjunto F^n asociado a la operación binaria de adición y a las operaciones singulares ω_λ, dicho de otra forma, el algebra $\langle F^n, +, \{\omega_\lambda |\ \lambda \in F\}\rangle$.

El espacio vectorial aritmético en n dimensiones sobre la estructura $\mathcal{F}$ se designa por el símbolo $\mathcal{F}^n$.

La operación de adición de vectores y operaciones simples ω_λ son las operaciones principales del espacio vectorial $\mathcal{F}^n$.

TEOREMA 1.1. *Las operaciones principales del espacio vectorial $\mathcal{F}^n$ están dotadas de las propiedades siguientes:*

(1) El algebra $\langle F^n, +, - \rangle$, donde $-a = \omega_{-1}$(a) *para cualquier* $\mathbb{a}$ de F^n, *es un grupo abeliano;*

(2) *La multiplicación para los escalares es asociativa, es decir, que $(\alpha\beta)\,\mathbb{a} = \mathbb{a}(\beta a)$ para cualquier α, β de F y cualquier $\mathbb{a}$ de F^n;*

(3) *La multiplicación por un escalar es distributiva en relación a la adición, es decir que $\alpha(a + b) = \alpha a + \alpha b$ para cualquier α, de F y cualquier a, b de F^n;*

(4) *La multiplicación para un vector es distributiva con respecto a la adición de escalares, es decir que $(\alpha + \beta)\, a = \alpha a + \beta a$ para cualquier α, β de F y cualquier a de F^n;*

(5) $1.a = a$ *para cualquier a de F^n.*

Demostración. Demostremos que el álgebra $\langle F^n, +, -\rangle$ es un grupo conmutativo. La conmutatividad de la adición de vectores se deriva directamente de la definición de la adición, así como el hecho que $\mathcal{F}$ es una estructura. La asociatividad de la adición se deduce de la asociatividad de adición de escalares.

$$(a+b)+c=\big((\alpha_1,\dots,\alpha_n)+(\beta_1,\dots,\beta_n)\big)+(\gamma_1,\dots,\gamma_n)=$$
$$=(\alpha_1+\beta_1,\dots,\alpha_n+\beta_n)+(\gamma_1,\dots,\gamma_n)=$$
$$=\big((\alpha_1+\beta_1)+\gamma_1,\dots,(\alpha_n+\beta_n)+\gamma_n\big)=$$
$$=\big(\alpha_1+(\beta_1+\gamma_1),\dots,\alpha_n+(\beta_n+\gamma_n)\big)=$$
$$=(\alpha_1,\dots,\alpha_n)+(\beta_1+\gamma_1,\dots,\beta_n+\gamma_n)=$$
$$=a+(b+v).$$

El vector 0 es un elemento neutro en relación a la adición, es decir que $a+0=0+a=a$ para todo vector a. El vector $-a=(-\alpha_1,\dots,-\alpha_n)$es el opuesto al vector a, es decir que $a+(-a)=0=(-a)+a$. $\langle F^n,+,-\rangle$ es entonces un grupo. Su conmutatividad se deduce de la conmutatividad de la adición de escalares.

Así mismo se verifica fácilmente el valor de las propiedades $(2)-(5)$. □

Dependencia e independencia lineales de un sistema de vectores.

Sean $\mathcal{F}$ una estructura escalar y F su conjunto de base. Sean $\mathcal{V}=\mathcal{F}^n$ un espacio vectorial aritmético en n dimensiones sobre $\mathcal{F}$ y $a_1,\dots,a_m$ un sistema cualquiera de vectores del espacio $\mathcal{V}$

DEFINICIÓN. Se denomina *combinación lineal del sistema de vectores* $a_1,\dots,a_m$ una suma de la forma $\lambda_1a_1+\cdots+\lambda_ma_m$ donde $\lambda_1,\dots,\lambda_m\in F$. Los escalares $\lambda_1,\dots,\lambda_m$ se denominan *coeficientes* de la *combinación lineal*. Una combinación lineal se denomina *no trivial* si al menos uno de sus coeficientes es diferente a cero. Sin embargo, este se denomina *trivial* si todos sus coeficientes son nulos.

DEFINICIÓN. El conjunto de todas las combinaciones lineales de los vectores del sistema $a_1,\dots,a_m$ se llama *envoltura lineal* de este sistema y se denota $L\,(a_1,\dots,a_m)$. La envoltura lineal de un sistema vacío es un conjunto compuesto del vector nulo.

En resumen, por definición,

$L(a_1,\dots,a_m)=\{\lambda_1a_1+\lambda_2a_2,\dots,+\lambda_ma_m|\ \lambda_1,\dots,\lambda_m\in F\}$.

Se constata sin problema que la envoltura lineal de un sistema dado de vectores está cerrados relativamente a las operaciones de adición de vectores y de multiplicación de vectores para los escalares.

DEFINICIÓN. Un sistema de vectores $a_1,\dots,a_m$ se denomina *linealmente independiente* (o libre) si para los escalares cualesquiera $\lambda_1,\dots,\lambda_m$ de la igualdad $\lambda_1a_1+\cdots+\lambda_ma_m=0$ se deducen las igualdades $\lambda_1=0,\dots,\lambda_m=0$. Un sistema de vectores vacíos se denomina linealmente independiente.

Dicho de otra manera, un sistema de vectores finitos es linealmente independiente si y sólo cualquier combinación lineal no trivial de vectores del sistema no es igual al vector nulo.

DEFINICIÓN. Un sistema de vectores $a_1,\dots,a_m$ se denomina *linealmente dependiente* (o asociado) si existe escalares $\lambda_1,\dots,\lambda_m$ no cualquier nulo, tal como,

$\lambda_1a_1+\cdots+\lambda_ma_m=0$.

Dicho de otra manera, un sistema de vectores finitos se denomina linealmente dependiente (asociado) si existe una combinación lineal no trivial de vectores del sistema igual al vector nulo.

El sistema de vectores

$e_1=(1,0,\dots,0),\quad e_2=(0,1,0,\dots,0),\dots,\ e_n=(0,0,\dots,0,1)$

se denomina *sistema de vectores unidos del espacio vectorial* $\mathcal{F}^n$. Este sistema de vectores es linealmente independiente. En efecto, para cualquier escalar $\lambda_1,\dots,\lambda_n$ de la igualdad $\lambda_1e_1+\cdots+\lambda_ne_n=0$ y por consiguiente, las igualdades $\lambda_1=0,\dots.,\lambda_n=0$.

Examínese las propiedades de dependencia e independencia lineales de un sistema de vectores.

PROPIEDAD 1.1. *Un sistema de vectores que contiene un vector nulo es linealmente dependiente.*

Demostración. Si en el sistema de vectores $a_1,\dots,a_k,\dots a_m$ es nulo, la combinación lineal de vectores del sistema, cuyos coeficientes son nulos, a excepción del coeficiente asociado a a_k, es entonces igual al vector nulo. Como resultado, un sistema de vectores es linealmente dependiente. □

PROPIEDAD 1.2. *Un sistema de vectores es linealmente dependiente si uno de sus subsistemas es linealmente dependiente.*

Demostración. Sea $a_1, \dots, a_k$, un subsistema linealmente dependiente que pertenece al sistema $a_1, \dots, a_m$, es decir que se obtiene $\lambda_1 a_1 + \cdots + \lambda_k a_k = 0$ con al menos uno de los coeficientes de $\lambda_1, \lambda_2, \dots, \lambda_k$ diferente de cero. Entonces $\lambda_1 a_2 + \cdots + \lambda_k a_k + 0.\, a_{k+1} + \cdots + 0.\, a_m = 0$. Así, el sistema de vectores $a_1, \dots, a_m$es linealmente independiente.□

Corolario. *Todo subsistema linealmente independiente es en sí mismo linealmente independiente.*

Propiedad 1.3. *El sistema de vectores*

(1) $u_1, u_2, \dots, u_m,$

en el cual $u_1 \neq 0$ *es linealmente dependiente si y sólo si al menos uno de los vectores* $u_2, \dots, u_m$ *constituye una combinación lineal de vectores antes mencionados*.

Demostración. Sea el sistema (1) linealmente dependiente y $u_1 \neq 0$. Existe en este caso escalares $\lambda_1, \dots, \lambda_m$ no para cualquiera nulo, tales como

(2) $\lambda_1 u_1 + \cdots \lambda_m u_m = 0$

Nótese k el más grande de los números $1,2, \dots, m$ que cumple con la condicione $\lambda_k \neq 0$. Se puede entonces escribir la igualdad (2) bajo la forma

(3) $\lambda_1 u_1 + \cdots + \lambda_k u_k = 0.$

Obsérvese que $k > 1$, ya que en el caso contrario $\lambda_2 = 0, \dots, \lambda_m = 0, \lambda_1 u_1 = 0$; así, $\lambda_1 = 0$, dado que $u_1 \neq 0$. Se deduce de (3) la igualdad

$$u_k = \left(-\lambda_k^{-1}\lambda_1\right)u_1 + \cdots + (-\lambda_k^{-1}\lambda_{k-1}) = u_{k-1}$$

Plantéese ahora que el vector $u_s, 1 < s \leq m$, es una combinación lineal de los vectores que le proceden, es decir que $u_s = \lambda_1 u_1 + \cdots + \lambda_{s-1} u_{s-1}$. Se obtiene entonces $\lambda_1 u_1 + \cdots + \lambda_{s-1} + (-1)u_s = 0$, dicho de otra manera, el subsistema $u_1, \dots, u_s$ del sistema (1) es linealmente dependiente. Como resultado, según la propiedad 1.2, el sistema de partida (1) es de igual manera linealmente dependiente. □

PROPIEDAD 1.4. *Si el sistema de vectores* $u_1, \dots, u_m$ *es linealmente independiente, mientras que el sistema de vectores*

(2) $U, U, \dots, U_{m,} V$

es linealmente dependiente, entonces el vector $\mathbb{v}$ *puede expresarse linealmente por medio de los vectores*

(1) $u_1, \dots, u_m,$

y de forma única.

Demostración. Por hipótesis el sistema (2) es linealmente dependiente, es decir que existe escalares $\lambda_1, \dots, \lambda_m, \lambda$ no para cualquier nulo, tales como

(3) $\lambda_1 u_1 + \cdots + \lambda_m u_m + \lambda_m = 0.$

Además $\lambda \neq 0$, ya que $\lambda = 0\ \lambda_1 u_1 + \cdots + \lambda_m u_m = 0$, lo cual es contradictorio con la independencia lineal del sistema (1). De (3) se deduce la igualdad

$$V = (-\lambda^{-1}\lambda_1) + \cdots + (-\lambda^{-1}\lambda_m)u_m.$$

Si $V = \lambda_1^{'}\mu_1 + \cdots + \lambda_m^{'} u_m\ y\ \ V = \mu_1 u_1 + \cdots + \mu_m u_m$, entonces

$$\left(\lambda_1^{'} - \mu_1\right)u_1 + \cdots + \left(\lambda_m^{'} - \mu_m\right)u_m = 0.$$

En virtud de la independencia lineal del sistema (1) se deduce que

$\lambda_1^{'} - \mu_1 = 0, \dots, \lambda_m^{'} - \mu_m = 0.\, y$

$$\lambda_1^{'} = \mu_1, \dots, \lambda_m^{'} = \mu_m. \square$$

PROPIEDAD 1.5. *Si* $u \in L(V_1, V_2, \dots, V_M)$ y $V_1, \dots, V_m \in L(W_1, \dots, w_s)$, *entonces se obtiene* $u \in L(w_1, \dots, w_s)$.

Demostración. La condición $u \in L(V_1, \ldots, V_m)$ significa que existen escalares $\alpha_1, \ldots, \alpha_m$ tales como

(1) $u = \alpha_1 V_1 + \cdots + \alpha_m V_m$.

La condición $V_i \in L(W_1, \ldots, W_s)$ significa que hay escalares $\lambda_{i\mathfrak{R}}$, tales como

(2) $V_i = \lambda_{i1} W_1 + \cdots + \lambda_{is} W_s \qquad (i = 1, \ldots, m)$.

En virtud de (1) y (2), se obtiene

$$u = \alpha_1(\lambda_{11} + \cdots + \lambda_{1s} W_s) + \cdots + \alpha_m(\lambda_{m1} + \cdots \ldots + \lambda_{ms} W_s) = (\alpha_1 \lambda_{11} + \cdots + \alpha_m \lambda_{m1}) W_1 + \cdots \ldots + (\alpha_1 \lambda_{1s} + \cdots + \alpha_m \lambda_{ms}) W_s,$$

es decir que $u \in L(W_1, \ldots, W_s)$. □

TEOREMA 1.2. *Si tenemos*

(1) $\mathbf{u}_1, \ldots, \mathbf{u}_{m+1} \in \boldsymbol{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{\boldsymbol{m}})$

el sistema de vectores $\mathbf{u}_1, \ldots, \mathbf{u}_{m+1}$ *es entonces linealmente dependiente.*

Demostración (se efectúa por inducción sobre m). Supóngase que los vectores $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m+1}$ no son nulos, ya que en el caso contrario el TEOREMA se vuelve evidente. Plantéese $m = 1$ y $\boldsymbol{u_1}, \boldsymbol{u_2} \in \boldsymbol{L}(\mathbb{v}_{\mathbf{1}})$, es decir que $\mathbf{u}_1 = \alpha \boldsymbol{v}_1$ y $\mathbf{u}_2 = \beta \boldsymbol{v}_1$. Entonces $\alpha \neq 0$, $\beta \neq 0$ y $\alpha^{-1}\mathbf{u}_1 + (-\beta^{-1})\mathbf{u}_2 = 0$. Por consiguiente, el sistema de vectores $\mathbf{u}_1$, $\mathbf{u}_2$ es linealmente dependiente.

Supóngase que el TEOREMA es verdadero para $m = n$ - 1 y demuéstrese que en este caso se verifica para $m = n$. Sea $\mathbf{u}_1, \ldots, \mathbf{u}_{n+1} \in \boldsymbol{L}(\boldsymbol{v}_1, \ldots, \boldsymbol{v_n})$, es decir que:

$$\mathbf{u_1} = \boldsymbol{\lambda_{11}}\mathbf{v_1} + \ldots + \boldsymbol{\lambda}_{1n}\mathbf{v}_n;$$

. . . . .

(2) $\mathbf{u}_n = \boldsymbol{\lambda}_{n1}\mathbf{v}_1 + \ldots + \boldsymbol{\lambda}_{nn}\mathbf{v}_n;$

$$\mathbf{u}_{n+1} = \boldsymbol{\lambda}_{n+1,\ 1}\mathbf{v}_1 + \ldots + \boldsymbol{\lambda}_{n+1,\ n}\mathbf{v}_n.$$

Si en los segundos grados de igualdad (2) todos los coeficientes asociados a $\mathbf{v}_n$ son nulos, entonces tenemos $\mathbf{u}_1, \ldots, \mathbf{u}_n \in \boldsymbol{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{\boldsymbol{n-1}})$, y que siguen la hipótesis de recurrencia el sistema de vectores $\mathbf{u}_1, \ldots, \mathbf{u}_n$ es linealmente dependiente y, por lo tanto, es el sistema $\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbf{u}_{n+1}$. Pero si al menos de uno de los coeficientes asociados a $\mathbf{v}_n$, por ejemplo $\boldsymbol{\lambda}_{n+1,\ n}$, es distinto a cero, entonces se excluye el vector $\mathbf{v}_n$ de n primeras igualdades. Y resulta así en:

$$\mathbf{u}_1 - \beta_1 \mathbf{u}_{n+1} = \boldsymbol{\lambda}'_{11}\mathbf{v_1} + \ldots + \boldsymbol{\lambda}'_{1,\ n-1}\mathbf{v}_{n-1}$$

. . . . . .

$$\mathbf{u}_n - \beta_n \mathbf{u}_{n+1} = \boldsymbol{\lambda}'_{n1}\mathbf{v}_1 + \ldots + \boldsymbol{\lambda}'_{n,\ n-1}\mathbf{v}_{n-1}$$

Siguiendo la hipótesis de recurrencia se deduce de (3) que el sistema de vectores $\mathbf{u}_1 - \beta_1 \mathbf{u}_{n+1}, \ldots, \mathbf{u}_n - \beta_n \mathbf{u}_{n+1}$ es linealmente dependiente. Existe así los escalares $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_n$ no cualquiera son nulos, tales como:

$$\boldsymbol{\lambda}_1(\mathbf{u}_1 - \boldsymbol{\beta}_1 \mathbf{u}_{n+1}) + \ldots + \boldsymbol{\lambda}_n(\mathbf{u}_n - \boldsymbol{\beta}_n \mathbf{u}_{n+1}) = 0$$

O

$$\boldsymbol{\lambda}_1\mathbf{u}_1 + \ldots + \boldsymbol{\lambda}_n\mathbf{u}_n + \boldsymbol{\lambda}_{n+1}\mathbf{u}_{n+1} = 0$$

donde $\boldsymbol{\lambda}_{n+1} = -\boldsymbol{\lambda}_1\boldsymbol{\beta}_1 + \ldots + \boldsymbol{\lambda}_n \boldsymbol{\beta}_n$). Por lo tanto, el sistema de vectores $\mathbf{u}_{1, \ldots,}\mathbf{u}_{n+1}$ es linealmente dependiente. □

COROLARIO 1.3. *Si* $\mathbf{u}_1, \ldots, \mathbf{u}_{\mathfrak{K}} \in \boldsymbol{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{\boldsymbol{m}})$ y $\kappa > m$, *entonces el sistema de vectores* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{\mathfrak{K}}$ *es linealmente dependiente.*

COROLARIO 1.4. *Si* $\mathbf{u}_1, \ldots, \mathbf{u}_{\mathfrak{K}} \in \boldsymbol{L}(\mathbf{v}_1, \ldots, \mathbf{v}_{\boldsymbol{m}})$ *y el sistema de vectores* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{\mathfrak{K}}$ *es linealmente independiente, entonces tenemos* $\kappa \leqslant m$.

COROLARIO 1.5. *En un espacio vectorial aritmético en n dimensiones cualquier sistema compuesto de* $n + 1$ *o más vectores es linealmente dependiente.*

El corolario 1.5 resulta del TEOREMA 1.2 dado que todo vector $(\alpha_1,\ldots,\alpha_n)$ en n dimensiones es una combinación lineal de unidad de vectores $\mathbf{e}_1,\ldots,\mathbf{e}_n$:

$$(\alpha_1,\ldots,\alpha_n) = \alpha_1\boldsymbol{e}_1+\ldots+\alpha_n\boldsymbol{e}_n \in \boldsymbol{L}\,(\boldsymbol{e}_1,\ldots,\boldsymbol{e}_n).$$

Sistemas de vectores equivalentes. Introdúzcase sobre un conjunto de sistemas finitos de vectores de un espacio vectorial dado $\boldsymbol{V}$ la operación binaria $\backsim$.

DEFINICIÓN. Sean S y T sistemas de vectores: $\boldsymbol{S} \backsim \boldsymbol{T}$ si cada vector no nulo de cualquiera de estos sistemas puede representarse bajo forma de una combinación lineal de vectores del otro sistema.

Verifíquese sin duda que la relación binaria $\backsim$ es reflexiva, transitiva y simétrica y, como consecuencia, es una relación de equivalencia. Por esta razón los sistemas de vectores $\boldsymbol{S}$ y $\boldsymbol{T}$ se denominan *equivalentes* si $\boldsymbol{S} \backsim \boldsymbol{T}$. Nótese que un sistema de vectores vacío es equivalente tanto a un sistema de vectores vacío como a un sistema compuesto de vectores nulos.

Considérese algunas propiedades de sistemas equivalentes de vectores.

TEOREMA1.6. *Dos sistemas de vectores son equivalentes si y solo si sus envolturas lineales son iguales.*

Demostración. Sea $\boldsymbol{S} \sim \boldsymbol{T}$. Cada vector del sistema S pertenece entonces al conjunto $\boldsymbol{L}\,(T)$, mientras que cada vector del sistema T pertenece al conjunto$\boldsymbol{L}\,(S)$. También en virtud de la propiedad 1.5 $\boldsymbol{L}\,(S) \subset \boldsymbol{L}\,(T)\ y\ \boldsymbol{L}\,(T) \subset \boldsymbol{L}\,(S)$, es decir $\boldsymbol{L}\,(S) = \boldsymbol{L}\,(T)$.

Recíprocamente: Si $\boldsymbol{L}\,(S) = \boldsymbol{L}\,(T)$, evidentemente tenemos $\boldsymbol{S} \sim \boldsymbol{T}$. □

TEOREMA1.7. *Si dos sistemas finitos de vectores son equivalentes y cada uno de ellos es linealmente independiente, entonces los dos sistemas se componen de un mismo número d vectores.*

Demostración. El TEOREMA es evidentemente verdadero si los dos sistemas de vectores son vacíos. Sean $\boldsymbol{u_1},\ldots,\boldsymbol{u_r}$ y $\boldsymbol{v_1},\ldots,\boldsymbol{v_s}$ dos sistemas equivalentes no vacíos, cada uno es linealmente independiente. En ese caso, en virtud del corolario 1.4, $r \leqslant s\ y\ s \leqslant r$. Por lo tanto, $r = s$. □

DEFINICIÓN. Denomínese *transformaciones elementales del sistema finito de vectores* a las transformaciones siguientes:

(α) la multiplicación de un vector cualquiera del sistema por un escalar no nulo;

(β)la adición (sustracción) a uno de los vectores del sistema de otro vector del sistema multiplicado por un escalar;

(γ) la exclusión del sistema o la inclusión en el sistema de un vector nulo.

Las transformaciones elementales (α) y (β) se denomina *regulares* y la transformación (γ) se llama *singular*.

TEOREMA 1.8. *Si uno de los sistemas finitos de vectores se obtiene de otro sistema de vectores después de una serie de transformaciones elementales, estos dos sistemas son equivalentes.*

Demostración. Sea

(1) $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$

el sistema de vectores de salida. Si se multiplica uno de los vectores de sistema, por ejemplo el primero, por un escalar $\boldsymbol{\lambda}$ diferente de cero, se obtiene el sistema $\boldsymbol{\lambda}\mathbf{a}_1, \ldots, \mathbf{a}_2, \ldots, \mathbf{a}_m$equivalente al sistema de salida.

Si se añade a uno de los vectores del sistema otro vector multiplicado por un escalar, por ejemplo, por adición al primer vector de un vector $\mathcal{K}$-ésimo multiplicado por $\boldsymbol{\lambda}$, se tiene un sistema $\mathbf{a}_1 + \boldsymbol{\lambda}\mathbf{a}_{\mathcal{R}}, \mathbf{a}_2, \ldots, \mathbf{a}_m$equivalente al sistema de salida.

Aplicando al sistema de vectores de salida la transformación (γ), aparentemente se acaba en el sistema de vectores equivalentes al sistema de salida. Como consecuencia, en virtud de la transitividad de la relación de equivalencia, el sistema de vectores, obtenido del sistema (1) por la serie de transformaciones elementales, es equivalente al sistema de vectores de salida (1). □

Base de un sistema finito de vectores. Introdúzcase una de las nociones fundamentales de la teoría de espacios vectoriales.

DEFINICIÓN. Se denomina *base de un sistema finito de vectores* a su sub-sistema no vacío linealmente independiente que le es equivalente.

Dicho de otro modo, la base de un sistema finito de vectores es su sub-sistema no vacío linealmente independiente mediante los vectores del cual se expresa linealmente cada uno de los vectores del sistema dado.

TOREMA 1.9. *Un sistema finito de vectores que contiene al menos un vector no nulo posee una base. Ambas bases de un sistema finito de vectores dados se componen de un mismo número de vectores.*

Demostración. Sea dado el sistema de vectores

(1) $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}}, \dots, \mathbf{u}_m$,

que contienen un vector nulo. Lo vectores nulos se pueden excluir del sistema (1), puesto que el sistema que se obtiene es equivalente al de salida. Se puede considerar que $\mathbf{u}_1 \neq 0$. Si el sistema (1) es linealmente independiente, es una base del sistema.

Si el sistema (1) es linealmente dependiente, entonces, en virtud de la propiedad 1.3, existe un vector, por ejemplo el vector $\mathbf{u}_{\mathcal{R}}$, igual a la combinación lineal de vectores que le precede. Por consecuencia, el sub-sistema:

(2) $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}-1}, \quad \mathbf{u}_{k+1}, \dots, \mathbf{u}_m$

es equivalente al sistema de salida y posee un vector no nulo. Si el sistema (2) es linealmente independiente, es una base del sistema (1). Pero si el sistema (2) es linealmente dependiente, se puede excluir del vector que constituye una combinación lineal de los vectores que lo preceden, etc. Después de un número finito de eliminaciones, se acaba en un sub-sistema de vectores en la cual ninguno se puede expresar linealmente por medio de vectores precedentes; este sub-sistema es la base del sistema (1), puesto que es linealmente independiente y no es vacío (contiene el vector $\mathbf{u}_1$).

Sean $\mathbf{v}_1, \dots, \mathbf{v}_{\mathrm{r}}$ y $\mathbf{w}_1, \dots, \mathbf{w}_s$ dos bases del sistema de vectores (1). Estas bases son equivalentes, puesto que cada una de ellas es equivalente al sistema (1). Por tanto, al seguir el TEOREMA 1.7, estas bases se componen de un mismo número de vectores, es decir que $r = s$. □

Rango de un sistema finito de vectores. Introdúzcase ahora la notación de rango de un sistema de vectores.

DEFINICIÓN. Denomínese *rango de un sistema finito de vectores* al número de vectores incluidos en una base cualquiera del sistema. El rango de un sistema de vectores nulos y el rango de un sistema de vectores vacíos son iguales a cero.

Considérese algunas propiedades del rango de un sistema de vectores.

TEOREMA 1.10. *Si* $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}} \in \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_m)$, *el rango de sistema de vectores* $u_1, \dots, u_k$ *es inferior o igual al rango del sistema de vectores* $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$.

Demostración. Si el primer sistema $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}}$ se compone de vectores nulos, su rango es entonces igual a cero y no sobrepasa el segundo sistema $\mathbf{v}_1, \dots, \mathbf{v}_m$. Supóngase que el primer sistema contiene por lo menos un vector no nulo. Entonces por hipótesis, se deduce que el segundo sistema posee igualmente vectores no nulos. Así que, según el TEOREMA 1.9, estos sistemas tienen cada uno una base. Supóngase que $\mathbf{u}_1, \dots, \mathbf{u}_{\mathrm{r}}$ es la base del primer sistema, mientras que $\mathbf{v}_1, \dots, \mathbf{v}_s$, es la base del segundo sistema. Pero entonces el sistema $\mathbf{v}_1, \dots, \mathbf{v}_s$es equivalente al sistema $\mathbf{v}_1, \dots, \mathbf{v}_m$ y en virtud del TEOREMA 1.6,

$$\boldsymbol{L}(\mathbf{v}_1, .., \mathbf{v}_m) = \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_s).$$

Además, por hipótesis, $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}} \in \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_m)$, por lo tanto $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}} \in \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_s)$.

Según el corolario 1.4 y en virtud de la independencia lineal del sistema de vectores $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}}$ resulta que $r \leqslant s$. Así que, el rango del primer sistema de vectores no es superior al del segundo sistema. □

PROPOSICIÓN 1.11. *El rango de cualquier sub-sistema del sistema finito de vectores no es superior al rango del sistema entero*.

Demostración. Esta afirmación es evidentemente verdadera si el sub-sistema es vacío. Si el sub-sistema no es vacío, la proposición 1.11 se deriva directamente del TEOREMA 1.10. □

PROPOSISCIÓN 1.12. Sistemas *finitos de vectores equivalentes tienen el mismo rango.*

Esta proposición se deriva del TEOREMA 1.10

PROPOSICIÓN 1.13*. El rango de cualquier sistema finito de vectores de un espacio vectorial aritmético en n dimensiones es inferior a n .*

Demostración. Sean $\mathbf{e}_{1, \dots,} \mathbf{e}_n$ los vectores unitarios del espacio vectorial aritmético $\mathcal{F}^{\mathrm{n}}$. Cualquier sistema $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{m}}$ los vectores de este espacio están contenidos en la envoltura lineal de los vectores unitarios $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{m}} \in \boldsymbol{L}(\mathbf{e}_{1, \dots,} \mathbf{e}_n) = F^{\mathrm{n}}$. Así que, en virtud del TEOREMA 1.10, el rango del sistema de vectores $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{m}}$ no puede sobrepasar n.□

PROPOSICIÓN 1.14. *Si un sistema finito de vectores posee el rango r, cualquier sub-sistema de este último compuesto de k vectores con $k > r$ es entonces linealmente dependiente.*

Demostración. Esta afirmación es aparentemente verdadera si el sistema está compuesto de vectores nulos. Plantéese que $\mathbf{v}_1, \dots, \mathbf{v}_m$ sea un sistema de vectores dado, $\mathbf{v}_1, \dots, \mathbf{v}_r$ su base, $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}}$ el sub-sistema de sistema dado, entonces se tienen

$$\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}} \in \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_r) = \boldsymbol{L}(\mathbf{v}_1, \dots, \mathbf{v}_m)$$

En virtud del corolario 1.3 para $k > r$ resulta que el sistema de vectores $\mathbf{u}_1, \dots, \mathbf{u}_{\mathcal{R}}$ es linealmente dependiente. □

PROPOSICIÓN 1.15. *Supóngase que el rango del sistema de vectores*

(1) $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{m}}$

Sea igual al rango del sistema de vectores

(2) $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{m}}, \ \mathbf{b}$.

Entonces se puede representar el vector $\boldsymbol{b}$ en forma de una combinación lineal de vectores del sistema (1).

Demostración. La proposición es evidentemente verdadera si los rangos del sistema (1) y (2) son iguales a cero. Supóngase que el rango r del sistema (1) es diferente a cero y $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{r}}$ es la base del sistema (1). Como por hipótesis, el rango del sistema (2) es también igual a r, su sub-sistema $\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{r}}, \ \mathbf{b}$ es linealmente dependiente. Resulta que, envirtud del corolario 1.4 que $\mathbf{b} \in \boldsymbol{L}(\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{r}})$. Así pues, $\mathbf{b} \in \boldsymbol{L}(\mathbf{a}_1, \dots, \mathbf{a}_{\boldsymbol{r}})$, dicho de otra manera, existen escalares $\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_m$ tales como

$$\mathbf{b} = \boldsymbol{\lambda}_1 \mathbf{a}_1 + \dots + \boldsymbol{\lambda}_m \mathbf{a}_{\boldsymbol{m}}. \ \square$$

Ejercicios

1. Sean (α, β) y (γ, δ) vectores del espacio $\mathcal{F}^2$. Demostrar que estos vectores son linealmente dependientes si y sólo si $\alpha\,\delta - \beta\,\gamma = 0$

2. Demostrar que los vectores aritméticos en n dimensiones $\mathbf{a}$ y $\mathbf{b}$ son linealmente dependientes si y sólo si $\mathbf{a}$ y $\mathbf{b}$ son proporcionales, es decir que para un escalar $\boldsymbol{\lambda}$ se tiene $\boldsymbol{a} = \boldsymbol{\lambda}\mathbf{b}$ o $\mathbf{b} = \boldsymbol{\lambda}\mathbf{a}$.

3. ¿A cuáles condiciones deben satisfacer los escalares β y γ para que los vectores (α, β) y $(\propto, \gamma)$ sean linealmente dependientes?

4. Demostrar que si en un sistema de vectores linealmente independientes $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}$, al agregársele a la derecha o izquierda un vector cualquiera $\mathbf{b}$, el sistema que se obtiene de un solo vector como máximo se expresará linealmente mediante los vectores que le preceden.

5. Sean $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}$ y $\mathbf{b}_1, \ldots, \mathbf{b}_{\boldsymbol{m}}$ dos sistemas de vectores linealmente independientes. Demostrar que si $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}} \in \boldsymbol{L}(\boldsymbol{b}1, \ldots, \boldsymbol{bm})$, entonces se tiene $\mathbf{b}_1, \ldots, \mathbf{b}_{\boldsymbol{m}} \in \boldsymbol{L}(\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}})$.

6. Sean $\mathcal{F} = \mathcal{Z}_2$ un cuerpo de clase residual módulo 2 y $\mathcal{V} = \mathcal{F}^n$. Demostrar que $\mathbf{a} + \mathbf{a} = \mathbf{0}$ para cualquier vector $\mathbf{a} \in \boldsymbol{V} = F^n$.

7. Sean $\mathcal{F} = \mathcal{Z}_3$ un cuerpo de clases residuales módulo 3 y $\mathcal{V} = \mathcal{F}^n$. Demostrar que $\mathbf{a} + \mathbf{a} + \mathbf{a} = \mathbf{0}$ para cualquier vector $\mathbf{a} \in \boldsymbol{V}$.

8. Sean $\mathcal{F} = \mathcal{Z}_3$ un cuerpo de clases residuales módulo 3 y n un entero positivo. ¿Cuántos vectores contiene el espacio vectorial $\mathcal{F}^n$?

9. ¿Cuándo un sistema de vectores posee una base única?

10. Demostrar que cualquier sub-sistema $\boldsymbol{r}$ de los vectores linealmente independiente de un sistema de vectores de rango $\boldsymbol{r}$ es una base del sistema.

11. Sea $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}$ un sistema de vectores linealmente independientes. Demostrar que $\mathbf{b} \in \boldsymbol{L}(\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}})$ si y sólo si el sistema de vectores $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}, \mathbf{b}$ es linealmente dependiente.

12. Demostrar que $\mathbf{b} \in \boldsymbol{L}(\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}})$ si y sólo si el rango del sistema de vectores $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}$ es igual al del sistema de vectores $\mathbf{a}_1, \ldots, \mathbf{a}_{\boldsymbol{m}}, \mathbf{b}$.

13. Demostrar que dos sistemas de vectores no vacíos equivalentes linealmente independientes encierran el mismo número de vectores.

14. Demostrar que si dos sistemas de vectores tiene un mismo rango y los vectores de un sistema se expresan linealmente en función de los vectores del otro, estos dos sistemas son equivalentes.

§ 2. Sistema de ecuaciones lineales

Implicaciones del sistema de ecuaciones lineales. En todo lo que sigue $\mathcal{F}$ es un cuerpo, un cuerpo de escalares.

DEFINICIÓN. Denomínese *sistema de ecuaciones lineales sobre el cuerpo $\mathcal{F}$ a variables $x_1, \ldots, x_{\mathrm{n}}$* el sistema de la forma

$$\begin{aligned} &\alpha_{11}x_1 + \cdots + \alpha_1 x_n = \beta_1 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n = \beta_m, \end{aligned}$$

donde $\alpha_{i\,\Re}, \beta_i \in F$.

Este sistema de m ecuaciones lineales se denotará bajo la forma

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \quad (i = 1, \ldots, m)$.

El sistema de ecuaciones lineales (1) constituye el predicado (la condición) en n variables libres $x_1, \ldots, x_{\mathrm{n}}$. Los valores específicos de las variables libres son considerados más adelante como elementos del cuerpo de escalares $\mathcal{F}$. Este predicado n-área es una conjunción de m predicados n-áreas definidos de forma más sencilla cada uno por una de las ecuaciones del sistema (1).

DEFINICIÓN. El vector $(\xi_1, \dots, \xi_n)$ de F^n se denomina *solución del sistema de ecuaciones* (1) si son verdaderas las igualdades

$$\alpha_{i1}\xi_1 +, \dots, +\alpha_{in}\xi_n = \beta_i \quad (i = 1, \dots, m).$$

DEFINICIÓN. Un sistema de ecuaciones lineales se denomina *compatible* si posee al menos una solución. Se denomina *incompatible* si es privado de soluciones, es decir que el conjunto de todas sus soluciones es vacío.

Junto al sistema (1) considérese el sistema (sobre $\mathcal{F}$)

(2) $\gamma_{i1}x_1 + \dots + \gamma_{in}x_n = \delta_i \quad (i = 1, \dots, s)$.

Nótese que un sistema de ecuaciones lineales puede contener solamente una ecuación.

DEFINICIÓN. El sistema de ecuaciones lineales (2) se dice *implicación del sistema de ecuaciones* (1) si cada solución del sistema (1) es igualmente una solución del sistema (2).

La notación $(1) \Longrightarrow (2)$ significa que el sistema (2) es una implicación del sistema (1).

Cualquier sistema de ecuaciones lineales (sobre $\mathcal{F}$) en n variables constituye una implicación del sistema de ecuaciones incompatibles (sobre $\mathcal{F}$) las mismas variables.

El sistema de ecuaciones lineales (2) es una implicación del sistema de ecuaciones (1) si y sólo si el conjunto de todas las soluciones del sistema (1) es un sub-conjunto del conjunto de todas las soluciones de (2).

Se constata sin duda que la relación binaria de implicación sobre un conjunto de sistemas de ecuaciones lineales (sobre $\mathcal{F}$) es reflexiva y transitiva, es decir una relación de pre-orden.

DEFINICIÓN. La ecuación lineal

$(\lambda_1\alpha_{11} + \dots + \lambda_m\alpha_{m1})x_1 + \dots + (\lambda_1\alpha_{1n} + \dots + \lambda_m\alpha_{mn})\, x_n = \lambda_1\beta_1 + \dots + \lambda_m\beta_m$, donde $\lambda_1, \dots, \lambda_m$ son elementos arbitrarios del cuerpo $\mathcal{F}$, se denomina *combinación lineal de ecuaciones del sistema* (1) con coeficientes $\lambda_1, \dots, \lambda_m$.

PROPOSICIÓN 2.1. *Cualquier combinación lineal de ecuaciones lineales del sistema de ecuaciones* (1) *es una implicación de este sistema.*

La demostración de esta proposición se deja al criterio del lector.

Sistemas equivalentes de ecuaciones lineales y transformaciones elementales del sistema. Más adelante se estudia los sistemas de ecuaciones lineales sobre el cuerpo $\mathcal{F}$ en n variables $x_1, \dots, x_n$.

DEFINICIÓN. Dos sistemas de ecuaciones lineales se llaman *equivalentes* si cada solución de cualquiera de estos sistemas es una solución del otro sistema.

Las proposiciones siguientes establecen las propiedades de la equivalencia derivándose la definición de equivalencia así como las propiedades antes mencionadas de la implicación de sistemas.

PROPOSICIÓN 2.2. *Dos sistemas de ecuaciones lineales son equivalentes si y sólo si cada uno de sus sistemas es una implicación del otro sistema.*

PROPOSICIÓN 2.3. *Dos sistemas de ecuaciones lineales son equivalentes si y sólo si el conjunto de todas las soluciones de uno de los sistemas coincide con el conjunto de todas las soluciones del otro sistema.*

PROPOSICIÓN 2.4. *Dos sistemas de ecuaciones lineales son equivalentes si y sólo si son equivalentes los predicados definidos por estos sistemas.*

DEFINICIÓN. Denomínese *transformaciones elementales de un sistema de ecuaciones lineales* a las transformaciones siguientes:

(α) la multiplicación de dos elementos de una ecuación cualquiera del sistema por un escalar es distinto a cero;

(β) la adición (la sustracción) a dos elementos de ecuación cualquiera del sistema de elementos que corresponde a otra ecuación del sistema multiplicado por un escalar;

(γ) la eliminación del sistema o la agregación al sistema de una ecuación lineal en coeficientes nulos y en término independiente nulo.

TEOREMA 2.5. *Si un sistema de ecuaciones lineales se obtiene de otro sistema de ecuaciones lineales al comienzo de una serie de transformaciones elementales, los dos sistemas son equivalentes.*

Demostración. Sea dado un sistema

$$\begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m. \end{aligned} \quad (1)$$

Si se multiplica una de sus ecuaciones, por ejemplo la primera por un escalar λ diferente a cero, se obtiene el sistema

$$\begin{aligned} &\lambda\alpha_{11}x_1+\ldots+\lambda\alpha_{1n}x_n=\lambda\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n=\beta_m. \end{aligned} \quad (2)$$

Cada solución del sistema (1) es igualmente una solución del sistema (2). Y recíprocamente: si $(\xi_1,\ldots,\xi_n)$ es una solución cualquiera del sistema (2), es decir

$$\begin{aligned} &\lambda\alpha_{11}x_1\xi_1+\ldots+\lambda\alpha_{1n}\xi_n=\lambda\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}\xi_1+\ldots+\alpha_{mn}\xi_n=\beta_m. \end{aligned}$$

entonces al multiplicar la primera igualdad por λ^{-1} y al no hacer variar las igualdades siguientes se obtienen las igualdades que demuestran que el vector $(\xi_1,\ldots,\xi_n)$ es una solución del sistema (1). Por lo tanto, el sistema (2) es equivalente al sistema inicial (1). De manera fácil también se verifica que al aplicar una sola vez al sistema (1) la transformación elemental (β) o (γ), se llega al sistema equivalente del sistema inicial (1). Dado que la relación de equivalencia es transitiva, una aplicación múltiple de transformaciones elementales da un sistema de ecuaciones equivalente al sistema inicial (1). □

COROLARIO 2.6. *Si a una de las ecuaciones del sistema de ecuaciones lineales se agrega una combinación lineal de otras ecuaciones del sistema, se llega a un sistema de ecuaciones equivalente al sistema de salida.*

COROLARIO 2.7. *Si se elimina del sistema de ecuaciones lineales o si se le agrega a este sistema una ecuación que constituye una combinación lineal de otras ecuaciones del sistema, entonces se obtiene un sistema de ecuaciones equivalente al de salida.*

Igualdad de rangos de filas y columnas de la matriz. Sea $\mathcal{F}$ un cuerpo. La tabla de la forma

$$A=\begin{bmatrix}\alpha_{11} & \cdots & \alpha_{1n}\\ \ldots & \ldots & \ldots\\ \alpha_{m1} & \cdots & \alpha_{mn}\end{bmatrix}, \quad (1)$$

donde $\alpha_{ik}\in \boldsymbol{F}$, se denomina *matriz* asociada a un cuerpo $\mathcal{F}$ o matriz $m\times n$ sobre $\mathcal{F}$. Introdúzcase las notaciones siguientes para las filas y las columnas de una matriz: la i-ésima fila de la matriz se denota de $A_i, A_i=[\alpha_{i1},\ldots,\alpha_{in}]$; la k-ésima columna de la matriz se denota A^k:

$$A^{\mathrm{k}}=\begin{bmatrix}\alpha_{ik}\\ \cdot\\ \cdot\\ \cdot\\ \alpha_{mk}\end{bmatrix}$$

Las filas de la matriz A pueden asimilarse en los vectores aritméticos en n dimensiones sobre $\mathcal{F}$. Las columnas de la matriz A pueden tomarse para los vectores en m dimensiones sobre $\mathcal{F}$.

DEFINICIÓN. Se denomina *rango de la fila de la matriz* A al rango del sistema de sus filas $A_1, \ldots, A_m$ asimilados a los vectores de n dimensiones sobre $\mathcal{F}$. Se llama *rango de la columna de la matriz* A al rango del sistema de sus columnas $A^1, \ldots, A^n$, tomadas para los vectores de m dimensiones sobre $\mathcal{F}$.

El rango de la fila de la matriz A se denota $r(A)$, la de la columna $\rho(A)$.

La matriz obtenida de la matriz A por sustitución en sus filas de las columnas correspondientes se dice *transpuesta* de A y se denota ${}^tA$,

$$ {}^tA = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{m1} \\ \ldots & \ldots & \ldots \\ \alpha_{1n} & \cdots & \alpha_{mn} \end{bmatrix}. $$

Por los símbolos $r({}^tA)$ y $\rho({}^tA)$ se designa respectivamente los rangos de filas y columnas de la matriz ${}^tA$.

Sea

$$ \begin{aligned} &\alpha_{11}x_1 + \ldots + \lambda\alpha_{1n}x_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0 \end{aligned} \tag{1} $$

un sistema homogéneo de ecuaciones lineales. La matriz A

$$ A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} $$

Se denomina *matriz* o *matriz fundamental* (o de base) *del sistema de ecuaciones* (1).

TEOREMA 2.8. *Si un sistema homogéneo de ecuaciones lineales sobre un cuerpo* $\mathcal{F}$

$$ \begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0 \end{aligned} \tag{1} $$

las variables $\lambda_1, \ldots, \lambda_n$ *es equivalente al sistema*

$$ \begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \end{aligned} \tag{2} $$

compuesta de las κ *primeras ecuaciones del sistema* (1), *los rangos de las columnas de las matrices de estos sistemas son entonces iguales.*

Demostración. Sean A y $\bar{A}$ las matrices de los sistemas de ecuaciones (1) y (2) respectivamente. Si $\bar{A}$ es una matriz nula, entonces todo vector de F^n es una solución del sistema (2). En virtud de la equivalencia de los sistemas (1) y (2), se deduce que cada vector de F^n es una solución del sistema (1). Por lo tanto, la matriz A es nula y su rango es cero.

Admítase ahora que $\bar{A}$ es una matriz no nula y que

$$ \bar{A}^1, \ldots, \bar{A}^r \tag{3} $$

es una base del sistema de columnas de la matriz $\bar{A}$. Entonces, en virtud de la equivalencia de los sistemas (1) y (2) el sistema $A^1, \ldots, A^r$ de r primeras columnas de la matríz A es linealmente independiente. Si $r < s \leqslant n$, el sistema de las columnas $A^1, \ldots, A^r, A^s$ es linealmente dependiente. En el caso contrario, en virtud de la equivalencia de (1) y (2) el

sistema $\bar{A}^1, \ldots, \bar{A}^r, \bar{A}^s$ de las columnas de la matriz $\bar{A}$ sería linealmente independiente, esto contradeciría la hipótesis (3). El sistema $A^1, \ldots, A^r$ es entonces la base del sistema de las columnas de la matríz A. Por tanto, los rangos de las columnas de las matrices A y $\bar{A}$ son los mismos. □

TEOREMA 2.9. *El rango de la fila de una matríz es igual al rango de su columna.*

Demostración. El TEOREMA es aparentemente verdadero para las matrices nulas. Supóngase que $A = \| \alpha_{ik} \|$ es una matriz no nula sobre el cuerpo $\mathcal{F}$ y que sus primeras filas r forman la base del sistema de filas de esta matriz. Considérese un sistema homogéneo de ecuaciones lineales sobre $\mathcal{F}$

$$\begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\quad\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0, \\ &\quad\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0 \end{aligned} \tag{1}$$

con respecto a las variables $\lambda_1, \ldots, \lambda_n$ para la cual A es una matriz.

Considérese igualmente un sistema homogéneo

$$\begin{aligned} &\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ &\quad\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0, \end{aligned} \tag{2}$$

compuesta de las primeras r ecuaciones del sistema (1); desígnese su matríz por $\bar{A}$. Como las r primeras filas de la matríz A constituyen la base del sistema de sus filas, cada ecuación del sistema (1) es entonces una combinación lineal de las ecuaciones del sistema (2). Por lo tanto, los sistemas de ecuaciones (1) y (2) son equivalentes. Según el TEOREMA 2.8 resulta de la equivalencia de los sistemas (1) y (2) la igualdad de los rangos de las columnas de las matrices de estos sistemas, es decir

$$\rho(A) = \rho(\bar{A}). \tag{3}$$

Ya que las columnas de la matriz $\bar{A}$ constituyen los vectores de r dimensiones sobre $\mathcal{F}$, según el corolario 1.6 $\rho(\bar{A}) \leqslant r = r(A)$ Por lo tanto, conforme a (3), se tiene

$$\rho(A) \leqslant r(A) \tag{4}$$

Una igualdad análoga se obtiene igualmente para la matriz transpuesta ${}^tA$, es decir que se tiene

$$\rho({}^tA) \leqslant r({}^tA). \tag{5}$$

Se ve fácilmente que $\rho({}^tA) = r(A)$, $r({}^tA) = \rho(A)$. De donde en virtud de (5), resulta

$$r(A) \leqslant \rho(A). \tag{6}$$

Sobre la base de (4) y (6) se concluye que $r(A) = \rho(A)$. □

Criterio de compatibilidad del sistema de ecuaciones lineales. Considérese un sistema de ecuaciones lineales sobre el cuerpo $\mathcal{F}$:

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m). \tag{1}$$

Las matrices

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \cdots & \cdots & \cdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n}\ \beta_1 \\ \cdots & \cdots & \cdots \\ \alpha_{m1} & \cdots & \alpha_{mn}\beta_m \end{bmatrix}$$

se denominan respectivamente *matrices fundamentales y completas* del sistema de ecuaciones (1). El vector $\mathbf{b}$

$$\mathbf{b} = \begin{bmatrix} \beta_1 \\ . \\ . \\ . \\ \beta_m \end{bmatrix}$$

Se denomina columna de términos libres.

Considérese la ecuación (sobre el cuerpo $\mathcal{F}$)

(2) $x_1 A^1 + \ldots + x_n A^n = \mathbf{b}$,

donde $A^1, \ldots, A^n$ es el vector columna de la matríz A.

TEOREMA 2.10. *La ecuación* (2) *es equivalente al sistema de ecuaciones* (1).

Demostración. Sea $(\xi_1, \ldots, \xi_n)$ cualquier solución del sistema (1), es decir

(3) $\alpha_{i1}\xi_1 + \cdots + \alpha_{in}\xi_n = \beta_i \qquad (i = m)$.

Teniendo en cuenta que

(4) $$\xi_1 A^1 + \cdots + \xi_n A^n = \begin{bmatrix} \alpha_{11}\,\xi_1 & \cdots & \alpha_{1n}\,\xi_n \\ \cdots & \cdots & \cdots \\ \alpha_{m1}\,\xi_1 & \cdots & \alpha_{mn}\,\xi_n \end{bmatrix}$$

las igualdades (3) pueden escribirse en una sola igualdad

$(2')$ $\xi_1 A^1 + \cdots + \xi_n A^n = \mathbf{b}$.

Y, recíprocamente: supóngase que el vector $(\xi_1, \ldots, \xi_n)$ es solución de la ecuación (2), es decir que se tiene la igualdad $(2')$. Entonces, en virtud de (4), a partir de $(2')$ resultan las igualdades (3). Así, cualquier solución de la ecuación (2) es solución del sistema (1). Por lo tanto, la ecuación (2) es equivalente al sistema de ecuación (1). □

COROLARIO 2.11. *Un sistema homogéneo de ecuaciones lineales*

$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$

es equivalente a la ecuación

$x_1 A^1 + \cdots + x_n A^n = 0$,

donde $\mathbf{0}$ *es el vector columna nulo en* m *dimensiones.*

La ecuación (2) *se denomina forma vectorial de notación del sistema de ecuaciones lineales* (1).

TEOREMA 2.12. *Sean* A *y* B *respectivamente las matrices fundamentales y completas del sistema de ecuaciones lineales* (1). *Las afirmaciones siguientes son equivalentes:*

I. El sistema de ecuaciones lineales (1) *es compatible.*

II. El ecuación (2) *admite una solución (sobre el cuerpo* $\mathcal{F}$*).*

III. El vector $\mathbf{b}$ *es un combinación lineal de las columnas de la matriz A, es decir* $\mathbf{b} \in \boldsymbol{L}(\mathrm{A}^1, \ldots, \mathrm{A}^n)$

IV. Los rangos de las columnas (de las filas) de las matrices A y B son iguales, $r(\mathrm{A}) = r(\mathrm{B})$

Demostración. En virtud del TEOREMA 2.10 la afirmación I conlleva la afirmación II.

Si la ecuación (2) tiene una solución, el vector $\mathbf{b}$ entonces puede representarse bajo la forma de una combinación lineal (con coeficientes del cuerpo $\mathcal{F}$) de las columnas de la matriz A. Por tanto, III se deduce de II.

Si $\mathbf{b} \in \boldsymbol{L}$ $(A^1, \ldots, A^n)$, el sistema de columnas $A^1, .., A^n$de la matriz A es equivalente al sistema de columnas $A^1, \ldots, A^n$, *b* de la matriz B. Según la proposición 1.12 eso conlleva la igualdad de los rangos de columnas de las matrices A y B. Por lo tanto, la afirmación III implica IV.

Supóngase que los rangos de columnas de las matrices A y B son los mismos. En este caso la base del sistema de columnas de la matriz A es también una base del sistema de columnas de la matriz B. Por lo tanto, $\mathbf{b} \in \boldsymbol{L}(A^1, \ldots, A^n)$, es decir que existen escalares $\lambda_1, .., \lambda_n \in \mathcal{F}$ tales como $\lambda_1 A^1 + \cdots + \lambda_n A^n = \mathbf{b}$. Esta última igualdad traduce que el vector $(\lambda_1, \ldots, \lambda_n)$ es solución de la ecuación (2) y, en virtud del TEOREMA 2.10, solución del sistema de ecuaciones (1). Así, la afirmación IV se deduce de la afirmación I. Por lo tanto, las afirmaciones I, II, III y IV son equivalentes. □

TOREMA 2.13 (DE KRONECKER-CAPELLI). *Un sistema de ecuaciones lineales es compatible si y solo si el rango de la matriz fundamental es igual al de la matriz completa.*

Este TEOREMA se deriva directamente del TEOREMA precedente.

COROLARIO 2.14. *Si el rango de la matriz de un sistema de ecuaciones lineales es igual al número de ecuaciones del sistema, este sistema de ecuaciones es compatible.*

Demostración. Sean A y B respectivamente matrices fundamental y completa del sistema de m ecuaciones lineales en n variables. Se tiene entonces $\rho(B) \geq \rho(A) = m$. Por otra parte, $\rho(B) \leqslant m$, puesto que la matríz B posee m filas. Como consecuencia, $\rho(B) = \rho(A)$. Así pues, según el TEOREMA 2.13, el sistema considerado de ecuaciones lineales es compatible. □

Conexión entre las soluciones de un sistema lineal no homogéneo y las soluciones de un sistema lineal homogéneo que se asocia. Sea dado un sistema lineal no homogéneo

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m)$

sobre el cuerpo $\mathcal{F}$. El sistema de ecuaciones lineales

(2) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$

se denomina *sistema homogéneo* asociado al sistema (1).

Sean $\boldsymbol{L}$ el conjunto de todas las soluciones del sistema homogéneo (2) y $\mathbf{c}$ una solución cualquiera del sistema (1). El conjunto $\{\mathbf{c} + \mathbf{d} \mid \mathbf{d} \in \boldsymbol{L}\}$ se denotará: $\mathbf{c} + \boldsymbol{L}$:

$$\mathbf{c} + \boldsymbol{L} = \{\mathbf{c} + \mathbf{d} \mid \mathbf{d} \in \boldsymbol{L}\}.$$

PROPOSICIÓN 2.15. *Si la solución del sistema no homogéneo* (1) *se añade a la solución del sistema homogéneo* (2), *se obtiene la solución del sistema* (1).

Demostración. Sean $(\gamma_1, \ldots, \gamma_n)$ la solución del sistema (1) y $(\delta_1, \ldots, \delta_n)$ la solución del sistema (2), dicho de otra manera,

$\alpha_{i1}\gamma_1 + \ldots + \alpha_{in}\gamma_n = \beta_i \qquad (i = 1, \ldots, m)$
$\alpha_{i1}\delta_1 + \ldots + \alpha_{in}\delta_n = 0 \qquad (i = 1, \ldots, m)$

Al sumar término a término estas igualdades se obtienen las igualdades

$$\alpha_{i1}(\gamma_1 + \delta_1)+\ldots+\alpha_{in}(\gamma_n + \delta_n) = \beta_i \qquad (i = 1, \ldots, m),$$

que muestran que el vector $(\gamma_1 + \delta_1, \ldots, \gamma_n + \delta_n)$ es una solución del sistema (1). □

PROPOSICIÓN 2.16. *La diferencia entre dos soluciones cualquieras del sistema no homogéneo de ecuaciones lineales es una solución del sistema asociado a él.*

Demostración. Sean $(\gamma_1, \ldots, \gamma_n)$ y $(\delta_1, \ldots, \delta_n)$ soluciones del sistema no homogéneo de ecuaciones (1), dicho de otra manera,

$$\alpha_{i1}\,\gamma_1 +\ldots+ \alpha_{in}\,\gamma_n = \beta_i \quad (i = 1,\ldots, m)$$

$$\alpha_{i1}\,\gamma'_1 +\ldots+ \alpha_{in}\,\gamma'_n = \beta_i \ (i = 1,\ldots, m)$$

Al sustraer término a término se llega a las igualdades

$$\alpha_{i1}\,(\gamma_1 - \gamma'_1) +\ldots+ \alpha_{in}\,(\gamma_n - \gamma'_n\,) = 0 \qquad (i = 1,\ldots, m),$$

que muestran que el vector $(\gamma_1 - \gamma'_1, \ldots, \gamma_n - \gamma'_n)$ es *solución del sistema homogéneo de ecuaciones* (2). □

TEOREMA 2.17. *Sean* $\boldsymbol{c}$ *la solución del sistema no homogéneo de ecuaciones lineales* (1) *y* $\boldsymbol{L}$ *el conjunto de todas las soluciones del sistema homogéneo* (2) *asociado al sistema. En este caso* $\boldsymbol{c} + \boldsymbol{L}$ *es el conjunto de todas las soluciones del sistema (1).*

Demostración. Sean $\boldsymbol{M}$ el conjunto de todas las soluciones del sistema (1) y $\mathbf{c} \in \boldsymbol{M}$**.** Cada elemento del conjunto $\mathbf{c} + \boldsymbol{L}$ puede representarse en forma de suma $\mathbf{c} + \mathbf{l}$, donde $\mathbf{l} \in \boldsymbol{L}$ **.**

En virtud de la proposición 2.15, $\mathbf{c} + \mathbf{l} \in \boldsymbol{M}$**.** Por lo tanto,

(3) $\mathbf{c} + \boldsymbol{L} \subset \boldsymbol{M}$**.**

La inclusión inversa es igualmente verdadera. En efecto, si $\mathbf{d}$ es una solución cualquiera del sistema (1), $\mathbf{c} \in \boldsymbol{M}$**,** entonces en virtud de la proposición 2.16, $\mathbf{d} - \mathbf{c} \in \boldsymbol{L}$**.** Por lo tanto, se tiene $\mathbf{d} \in \mathbf{c} + \boldsymbol{L}$; por consiguiente,

(4) $\boldsymbol{M} \subset \mathbf{c} + \boldsymbol{L}$**.**

Sobre la base de (3) y (4) se concluye que $\boldsymbol{M} = \mathbf{c} + \boldsymbol{L}$**.** □

COROLARIO 2.18. *Un sistema de ecuaciones lineales no homogéneo compatible admite una solución única si y sólo si el sistema de ecuaciones homogéneo que se le asocia tiene una solución única (nula).*

COROLARIO 2.19. *Si dos sistemas no homogéneos de ecuaciones lineales (sobre el cuerpo*$\mathcal{F}$*) en* n *variables* $x_1, \ldots, x_n$ son compatibles y equivalentes, los sistemas homogéneos de ecuaciones que se les asocia son igualmente equivalentes.

TEOREMAs implicados por un sistema de ecuaciones lineales. Considérese el sistema de ecuaciones lineales

(I) $\alpha_{i1}x_1+\ldots+ \alpha_{in}x_n = \beta_i \qquad (i = 1,\ldots, m)$

sobre el cuerpo $\mathcal{F}$. La ecuación lineal

(II) $\gamma_1\, x_1 +\ldots+ \gamma_n\, x_n = \beta,$

donde $\gamma_1, \ldots, \gamma_n \in \boldsymbol{F}$ se denomina implicación del sistema (I) si cada solución del sistema (I) es solución de esta ecuación.

Según la proposición 2.1, toda combinación lineal (con coeficientes del cuerpo $\mathcal{F}$) de ecuaciones del sistema (I) es una implicación de ese sistema. ¿Es la recíproca verdadera? La respuesta a esta pregunta se proporciona por los TEOREMAs siguientes.

TEOREMA 2.20. *La ecuación lineal*

(2) $\gamma_1\, x_1 +\ldots+ \gamma_n\, x_n = 0,$

que es una implicación del sistema homogéneo de ecuaciones

(1) $\alpha_{i1}x_1+\ldots+\alpha_{in}x_n = 0\ (i = 1,\ldots, m)$,

constituye una combinación lineal de ecuaciones lineales de este sistema.

Demostración. Por hipótesis, la ecuación (2) es la implicación del sistema (1). Por lo tanto, el sistema

$$\alpha_{11}x_1+\ldots+\alpha_{1n}x_n = 0,$$

(3) . . . . . .

$$\alpha_{11}x_1+\ldots+\alpha_{1n}x_n = 0,$$
$$\gamma_1 x_1 +\ldots+ \gamma_n x_n = 0$$

es equivalente al sistema (1). Según los TEOREMAs 2.8 y 2.9 se deduce que el rango de la matriz A del sistema (1) es igual al de la matriz $\bar{A}$ del sistema (3). Por ello si $\mathbf{c} = (\gamma_1, \ldots, \gamma_n)$, se tiene

rango $\{A_1, \ldots, A_m, \mathbf{c}\}$ = rango $\{A_1, \ldots, A_m\}$,

donde A_i es la i – ésima fila de la matríz A. Sobre la base de esta igualdad se concluye que $\mathbf{c}$ es una combinación lineal de las filas $A_1, \ldots, A_m$ de la matríz A. Por consiguiente, la ecuación (2) es una combinación lineal de ecuaciones del sistema (1). □

TEOREMA 2.21. *Dos sistemas homogéneos de ecuaciones lineales sobre el cuerpo* $\mathcal{F}$ en n *variables* $x_1, \ldots, x_n$ *son equivalentes si y sólo si las matrices de estos sistemas son equivalentes por filas.*

Este TEOREMA se deduce fácilmente del TEOREMA 2.20.

TEOREMA 2.22. *Una ecuación lineal que constituye una implicación de un sistema compatible de ecuaciones lineales es una combinación lineal de ecuaciones de este sistema.*

Demostración. Admítase que la ecuación (II) es una implicación del sistema compatible (I). En este caso, el sistema de ecuaciones

$$\alpha_{11}x_1+\ldots+\alpha_{1n}x_n = \beta_1,$$

(4) . . . . . .

$$\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n = \beta_m,$$
$$\gamma_1 x_1 +\ldots+ \gamma_n x_n = \beta$$

es compatible y equivalente al sistema (1). Según el corolario 2.19 se deduce una equivalencia de sistemas homogéneos apropiados, es decir que el sistema de ecuaciones

(4) $\alpha_{i1}x_1+\ldots+\alpha_{in}x_n = 0\ (i = 1,\ldots, m)$,

es equivalente al sistema de ecuaciones

$$\alpha_{11}x_1+\ldots+\alpha_{1n}x_n = 0,$$

(5) . . . . . .

$$\alpha_{m1}x_1+\ldots+\alpha_{mn}x_n = 0,$$
$$\gamma_1 x_1+\ldots+\gamma_n x_n = 0.$$

Conforme a los TEOREMAs 2.8 y 2.9 el rango de la matriz A del sistema (4) es igual al rango de la matriz $\bar{A}$ del sistema (5). Por lo tanto, los rangos de las matrices fundamentales de los sistema (1) y (3) son iguales. Como los sistemas (1) y (3) son compatibles, según el criterio de compatibilidad, se deduce que el rango de las filas de la matriz completa B

del sistema (1) es igual al rango de las filas de la matriz completa $\bar{B}$ del sistema (3). Al apoyarse sobre la igualdad de estos rangos se concluye que la última fila de la matriz $\bar{B}$ es una combinación lineal de las filas de la matriz B, es decir que

$$(\gamma_1, \ldots, \gamma_n, \beta) \in \boldsymbol{L}(B_1, \ldots, B_n).$$

Por consiguiente, la ecuación (II) es una combinación lineal de ecuaciones del sistema (I). □

Ejercicios

1. Sea A una matriz $n \times m$ en filas linealmente independientes. Demostrar que $m \geq n$.

2. Demostrar que el rango r de una matriz $m \geq n$ no es superior a m y $n, r \leqslant \min(m, n)$

3. Demostrar que al eliminar una fila (una columna) en una matriz, no se modifica su rango si y sólo si la fila (columna) eliminada se expresa linealmente en función de las otras líneas (columnas).

4. Demostrar que la agregación en una matriz de una fila (de una columna) no modificaría su rango o aumentaría una unidad.

5. Demostrar que si el rango de la matriz A no varía después de añadir a esta última una columna cualquiera de la matriz B al mismo número de filas, este rango no varía lo mismo después de añadirlo a la matriz A de cualquiera de las columnas de la matriz B.

6. Supóngase que la matriz B se obtiene a partir de la matriz A por una serie de transformaciones lineales regulares de las filas. Demostrar que las filas de la matriz A son linealmente independientes si y sólo si las filas de la matriz B son linealmente independientes.

7. Sean A y B matrices en n columnas. Demostrar que las matrices A y B son equivalentes por filas en caso de que la envoltura lineal de las filas de la matriz A coincidan con la envoltura lineal de las filas de la matriz B.

8. Sean A una matriz $m \times n$ y B una matriz $m \times (n + \kappa)$ obtenida a partir de la matriz A por añadidura de κ columnas nuevas. Demostrar que

(a) si las filas de la matriz B son linealmente dependientes, las filas de la matriz A también lo son:

(b) si las filas de la matriz A son linealmente independientes, las filas de la matriz B también lo son;

(c) el rango de la matriz A no es superior al de la matriz B.

9. El rango de la matriz de un sistema homogéneo de ecuaciones lineales es inferior de una unidad al número de variables. Demostrar que las dos soluciones de este sistema son proporcionales (es decir que no se distingue solo de un factor escalar).

10. Buscar las condiciones para las cuales con cualquier solución de un sistema homogéneo de ecuaciones lineales la κ – ésima variable es nula.

11. Demostrar que si un sistema de ecuaciones lineales sobre el cuerpo Q de los números racionales no tiene soluciones en Q, no posee soluciones en cualquier cuerpo numérico.

12. Sea dado el sistema homogéneo de ecuaciones lineales (1) (sobre el cuerpo Q de los números racionales) que poseen soluciones no nulas. Cualquier sistema fundamental de las soluciones del sistema (1) sobre Q es un sistema fundamental sobre todo cuerpo numérico.

13. Sea

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \quad (i = 1, \ldots, m)$

Un sistema homogéneo de ecuaciones lineales (sobre el cuerpo $\mathcal{F}$). Demostrar que la ecuación

$\beta_1 x_1 + \ldots + \beta_n x_n = 0$

Es una implicación del sistema (1) si y sólo si es una combinación lineal de ecuaciones (1).

§ 3. Matrices escalares y sistemas de ecuaciones lineales

Matrices escalares. Sea

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix}$$

la matriz $m \times n$ sobre el cuerpo $\mathcal{F}$. *El elemento pivote de la fila de la matriz* es su primer elemento (al contar a partir de la izquierda) no nulo. La columna de la matriz se denomina *fundamental* si contiene el elemento pivote de una fila cualquiera de la matriz.

DEFINICIÓN. La matriz A se denomina *escalar* si satisface a las condiciones:

(1) las filas en elementos nulos (si existen) se hallan por debajo de todas las líneas en elementos no nulos;

(2) si $\alpha_{1k1}, \alpha_{2k2}, \ldots, \alpha_{rkr}$ son elementos pivotes de las filas en elementos no nulos de la matriz. Entonces $\kappa_1 < \kappa_2 < \ldots < \kappa_r$.

Ejemplos de matrices escalares: 1) la matriz nula, 2) la matriz unifila, 3) la matriz unidad, 4) la matriz triangular superior

$$\begin{bmatrix} \alpha_{11} & \alpha_{22} & \ldots & \alpha_{1n} \\ 0 & \alpha_{12} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_{nn} \end{bmatrix}.$$

Al sistema de vectores filas (columnas) de esta matriz se les puede aplicar las transformaciones elementales.

DEFINICIÓN. Las transformaciones elementales sobre un sistema de filas (columnas) de una matriz se llaman *transformaciones elementales de la matriz*. Dos matrices se denominan *equivalentes por filas* si una se obtiene a partir de la otra por una de serie de transformaciones elementales sobre las filas.

La relación de equivalencia por filas es reflexiva, simétrica y transitiva, es decir es una relación de equivalencia.

DEFINICIÓN. Se denomina *rango de fila de la matriz* al rango del sistema de sus filas. Se denomina *rango de columna de la matriz* al rango del sistema de sus columnas.

De esta definición, en virtud del TEOREMA 1.8, se deduce la proposición 3.1.

PROPOSICIÓN 3.1. *Si una matríz se obtiene de otra por medio de una serie de transformaciones elementales sobre filas, entonces los rangos de fila de esa matriz son iguales.*

TEOREMA 3.2. *Cualquier matiz $m \times n$ es equivalente por filas a una matriz escalar $m \times n$.*

Demostración (por inducción sobre el número de filas de la matriz). Si el número de filas de la matriz es igual a la unidad, entonces la matriz es escalar. Al plantear que el TEOREMA es verdadero para las matrices en $m - 1$ filas, demuéstrese que es también verdadero para las matrices en m filas. Sea A un matriz en m filas:

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{22} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{12} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{bmatrix}.$$

Si en la primera columna de la matriz se tiene un elemento diferente de cero, se puede permutar la fila con este elemento no nulo y la primera fila. Se muestra fácilmente que una permutación de filas es la conclusión de una serie de transformaciones elementales sobre filas. Por consiguiente se admitirá que $\alpha_{11} \neq 0$. La matriz A puede transformarse en la matriz B:

$$B = \begin{bmatrix} 1 & \beta_{12} & \ldots & \beta_{1n} \\ 0 & \beta_{22} & \ldots & \beta_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \beta_{m2} & \ldots & \beta_{nn} \end{bmatrix}$$

por una serie de transformaciones elementales. Para ello la primera fila de la matriz A debe multiplicarse por α_{11}^{-1}. A continuación, la primera fila obtenida se multiplica por $(-\alpha_{i\Re})$, se agrega a la i – ésima fila para $i = 2, \ldots, m$. La matriz formada a partir de B por eliminación de la primera fila incluye $m - 1$ filas y, por hipótesis de inducción, es equivalente por filas en una cierta matriz $(m - 1) \times n$ en escalar *C*:*

$$\begin{bmatrix} 0 & \beta_{12} \ldots & \beta_{1n} \\ \ldots & \ldots & \ldots \\ 0 & \beta_{m2} \ldots & \beta_{mn} \end{bmatrix} \sim C^* = \begin{bmatrix} 0 & \gamma_{22} \ldots & \gamma_{2n} \\ \ldots & \ldots & \ldots \\ 0 & \gamma_{m2} \ldots & \gamma_{mn} \end{bmatrix}.$$

Al apoyarse en este hecho, así como sobre la equivalencia por filas de las matrices A y B, se puede concluir que la matriz A es equivalente por filas a la matriz escalar C:

$$C = \begin{bmatrix} 1 & \beta_{12} \ldots \beta_{1n} \\ 0 & \gamma_{22} \cdots \gamma_{2n} \\ \ldots & \ldots \ldots \\ 0 & \gamma_{m2} \cdots \gamma_{mn} \end{bmatrix}.$$

La matriz C es escalar dado que la matriz C^* lo es también.

Si la primera columna o varias primeras columnas de la matriz Atienen en todas partes ceros, se considerará la matriz obtenida por eliminación de estas columnas. Esta matriz implica en la primera columna un elemento no nulo. Se deduce por lo tanto de la primera parte de la demostración que esta matriz es equivalente por filas a una matriz escalar. Se constata inmediatamente que al agregar a la derecha esta matriz escalar las columnas en elementos en todas partes nulos eliminados anteriormente, resulta en una matriz equivalente por filas en la matriz de salida A. □

TEOREMA 3.3. *El rango de filas de una matriz en escalar es igual al número de sus filas a CON elementos no nulos.*

DEMOSTRACIÓN. El TEOREMA es aparentemente verdadero para una matriz nula. Supóngase que A es una matriz escalar de r filas en elementos no nulos. Por conveniencia de escritura se plantea que los elementos pivotes de la matriz A ocupa las r primeras columnas, dicho de otra manera,

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} \ldots & \alpha_{1r} \ldots \\ 0 & \alpha_{22} \ldots & \alpha_{2r} \ldots \\ \ldots & \ldots & \ldots \\ 0 & 0 \ldots & \alpha_{rr} \ldots \\ 0 & 0 \ldots 0 \ldots & \end{bmatrix},$$

donde $\alpha_{11} \neq 0$ para $i = 1,\ldots, r$. Así, las r primeras filas $A_1, \ldots, A_r$ de la matriz A no tienen de manera uniforme ceros, mientras que las otras (si existen) tienen de manera uniforme ceros. Muéstrese que las filas $A_1,\ldots,A_r$ son linealmente independientes. Es necesario mostrar que para todo los escalares $\lambda_1 + \ldots + \lambda_r$ de la igualdad

$\lambda_1 A_1 + \ldots + \lambda_r A_r = 0$

Se derivan las igualdades

(2) $\lambda_1 = 0,\ldots, \lambda_r = 0$

Dado que

$\lambda_1 A_1 + \ldots + \lambda_r A_r =$

$= (\lambda_1 \alpha_{11}, \lambda_1 \alpha_{12} + \lambda_2 \alpha_{22}, \ldots, \lambda_1 \alpha_{1r} + \ldots + \lambda_r \alpha_{rr}, \ldots),$

De (1) se derivan las igualdades

$\lambda_1\alpha_{11} = 0,$

$\lambda_1\alpha_{12} + \lambda_2\alpha_{22} = 0,$

(3) . . . . . .

$\lambda_1\alpha_{1r} + \ldots + \lambda_r\alpha_{rr} = 0.$

Ya que $\alpha_{ii} \neq 0$ para $i = 1, \ldots, r$ de (3) se derivan las igualdades (2). Entonces, el sistema $A_1, \ldots, A_r$ de filas con elementos para todos no nulos en la matriz A es linealmente independiente. Por lo tanto, el rango de fila de la matriz A vale r. En caso general la demostración se efectúa de manera análoga.□

Apoyándose en el TEOREMA 3.3 Se llega a la regla de cálculo siguiente del rango de la matriz. *Para calcular el rango de fila de la matriz A es necesario reducirla a la forma escalonada C por una serie de transformaciones elementales en las filas. El número de filas en elementos no nulos en la matriz C es igual al rango de las filas de la matriz A*.

Matrices reducidas por escalones. Durante la resolución y el estudio de un sistema de ecuaciones lineales un rol importante corresponde a las matrices reducidas por escalones.

DEFINICIÓN. Una matriz escalar se llama *reducida* si la matriz compuesta de todas sus columnas fundamentales es una matriz identidad.

Una matriz reducida por escalones no posee filas, en elementos para todos nulos y todos sus elementos pivotes de sus filas son iguales a la identidad.

TEOREMA 3.4. *Toda matriz no nula es equivalente por fila a la matriz reducida por escalones.*

Demostración. Sea A una matriz no nula de rango r. Según los TEOREMAs 3.2 y 3.3 la matriz es equivalente por fila a la matriz escalar, por ejemplo, en la matriz B compuesta de r filas en elementos no nulos. Divídase cada fila de la matriz B por su elemento pivote. Se llega a una matriz C escalonada de la cual todos los elementos pivote de las filas son iguales a la identidad. Por secuencia de una serie de transformaciones elementales de filas en la matriz C son igual a cero, todos los elementos no nulos se colocan debajo de los elementos pivote. Se obtiene una matriz D cuyas columnas fundamentales constituyen la matriz identidad. Por lo tanto D es la matriz reducida por escalones buscada que es equivalente por fila a la matriz inicial A.□

TEOREMA 3.5 *Toda matriz cuadrada $n \times n$ en filas linealmente independientes es equivalente por fila a la matriz identidad $n \times n$ E.*

Demostración. Sea A la matriz $n \times n$ en filas linealmente independiente. En medio de una serie de transformaciones elementales regulares las filas se pueden reducir a una matriz $n \times n$ en escalar $C = \| \gamma_k \|$. Sean $\gamma_{1k1}, \gamma_{2k2}, \ldots, \gamma_{nkn}$ los elementos pivotes de la matriz C. Entonces se tiene

(1) $\gamma_{1k_1} \neq 0, \ldots, \gamma_{nk_n} \neq 0$

(2) $1 \leq \mathcal{K}_1 < \mathcal{K}_2 < \ldots < \mathcal{K}_n \leq n$.

De las desigualdades (2) se deduce que $\mathcal{K}_1 = \mathbf{1}, \mathcal{K}_2 = 2, \ldots \mathcal{K}_n = \boldsymbol{n}$.

Por lo tanto la matriz C es de la forma:

$$C = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1n} \\ 0 & \gamma_{22} & \cdots & \gamma_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \gamma_{nn} \end{bmatrix}$$

Dicho de otra manera, es una matriz triangular superior en elementos nulos sobre la diagonal principal. Multiplíquese la primera fila de la matriz porγ_{11}^{-1}, la segunda por γ_{22}^{-1}entre otros. Se llega así a una matriz equivalente por filas:

$$C' = \begin{bmatrix} 1 & \gamma'_{12} & \dots & \gamma'_{1n} \\ 0 & 1 & \dots & \gamma'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Se constata sin duda que la matriz C' es equivalente por fila a la matriz identidad $n \times nE$. Entonces existe una serie de transformaciones elementales (regulares) de filas que reducen la matriz A en una matriz de identidad E. □

Sistema homogéneo de ecuaciones lineales. Considérese un sistema homogéneo de ecuaciones en el cuerpo$\mathcal{F}$.

$$\begin{aligned} &\alpha_{11}x_1 + \dots + \alpha_{1n}x_n = 0\,, \\ &\dots\dots\dots\dots\dots\dots \\ &\alpha_{m1}x_1 + \dots + \alpha_{mn}x_n = 0. \end{aligned} \qquad (1)$$

Sea

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{\mathbf{11}} & \dots & \boldsymbol{\alpha_{1n}} \\ \dots & \dots & \dots \\ \boldsymbol{\alpha_{m1}} & \dots & \boldsymbol{\alpha_{mn}} \end{bmatrix}$$

Una matriz compuesta de coeficientes vinculados a las variables y llamada *matrices fundamentales del sistema* (1),A^1, . . . ,A^n siendo las columnas de esta matriz .La ecuación (en $\mathcal{F}$)

$$x_1\boldsymbol{A^1} + \dots + x_n\boldsymbol{A^n} = \mathbf{0}, \qquad (2)$$

Donde **0** es el vector columna nulo se llama *forma vectorial de escritura del sistema de ecuaciones (1)*.

Según el corolario 2.11 un sistema homogéneo de ecuaciones (1) es equipotente a la ecuación (2).

PROPOCISION 3.6. *Si la matriz A de un sistema homogéneo de ecuaciones* (1) *posee el rango $rr >$ $0\ y\ A_1,\ \dots\ , A_r$ es la base del sistema de sus líneas, el sistema (1) es entonces equipotente al sistema*

$$\begin{aligned} &\alpha_{11}x_1 + \dots + \alpha_{1n}x_n = 0\,, \\ &\dots\dots\dots\dots\dots\dots \\ &\alpha_{r1}x_1 + \dots + \alpha_{rn}x_n = 0\,, \end{aligned} \qquad (3)$$

Compuesta de r primeras ecuaciones del sistema (1).

Demostración. Dado que las r primeras filas de la matriz A constituyen la base del sistema de filas en esta matriz, cada ecuación del sistema (1) es por lo tanto una combinación lineal de ecuaciones (3). Además el sistema (3) es una implicación del sistema (1). Por lo tanto, los sistemas (1) y (3) son equipotentes.□

PROPOSICION 3.7. *Un sistema homogéneo de ecuaciones lineales de la matriz A posee las soluciones no nulas si y solo si las columnas de la matriz A son linealmente dependientes.*

Esta proposición se deriva directamente del corolario 2.11.

COROLARIO3.8. *Un sistema homogéneo de ecuaciones lineales en n variables posee las soluciones no nulas si y solo si el rango de la matriz del sistema es inferior a n.*

COROLARIO3.9. *Si el número de ecuaciones de un sistema homogéneo de ecuaciones lineales es inferior al número de variables, el sistema tienes soluciones no nulas.*

PROPOCISION 3.10. *El conjunto de todas las soluciones de un sistema homogéneo de ecuaciones lineales es cerrado en relación a la adición, sustracción y multiplicación por los escalares .Toda combinación lineal de soluciones de un sistema homogéneo de ecuaciones es una solución de ese sistema.*

La demostración de la proposición 3.10 se deja a opción del lector.

Sistema fundamental de soluciones. Sea

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1,\ldots,m)$$

un sistema homogéneo de ecuaciones lineales en el cuerpo $\mathcal{F}$.

DEFINICIÓN. Se llama *sistema fundamental de soluciones del sistema de ecuaciones* (1) el sistema no vacío linealmente independiente de sus soluciones cuya envoltura lineal coincide con el conjunto de todas las soluciones del sistema (1).

Nótese que el sistema homogéneo de ecuaciones lineales que no posee una solución nula no tiene el sistema fundamental de soluciones.

PROPOSICIÓN 3.11. *Dos sistemas fundamentales cualesquiera de soluciones del sistema homogéneo de ecuaciones lineales admiten un mismo número de soluciones.*

Demostración. De hecho, dos sistemas fundamentales cualesquiera de las soluciones del sistema homogéneo de ecuaciones (1) son equivalentes y linealmente independientes. En este caso conforme a la proposición 1.12 sus rangos son iguales. Por lo tanto el número de soluciones que entra en uno de los sistemas fundamentales es igual al número de soluciones que componen el otro sistema fundamental de soluciones.□

Si la matriz A de un sistema homogéneo de ecuaciones (1) es nula, entonces todo vector de F^n es solución del sistema **(1)**; en este caso toda colección de n vectores linealmente independientes de F^n es un sistema fundamental de soluciones. Pero si el rango de la columna de la matriz A es n, el sistema (1) entonces no admite más que una solución, la solución nula; por tanto en este caso el sistema de ecuaciones (1) es destituido del sistema fundamental de soluciones.

TEOREMA 3.12.*Si el rango r de la matriz de un sistema homogéneo de ecuaciones lineales (1) es inferior al número de variables n el sistema (1) entonces tiene un sistema fundamental de soluciones que contiene $n - r$ soluciones.*

Demostración. Si el rango de la matriz fundamental A del sistema homogéneo (1) es igual a cero o a n entonces el TEOREMA es verdadero, como se mostró anteriormente. Es por eso que se admite más adelante que $0 < r(A) < n$. Al plantear $r = r(A)$, se supondrá que las r primeras columnas de la matriz A son linealmente independientes. En este caso la matriz A es equivalente por fila a la matriz reducida por escalones, mientras que el sistema (1) es equivalente al sistema de ecuaciones reducida por escalones de la forma:

$$\begin{aligned} x_1 - \quad & \ldots - \gamma_{11}x_{r+1} - \ldots - \gamma_{1,n-r}x_n = 0, \\ x_2 - \ldots & - \gamma_{21}x_{r+1} - \ldots - \gamma_{2,n-r}x_n = 0, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r - \gamma_{r1}x_{r+1} - \ldots & - \gamma_{r,n-r}x_n = 0. \end{aligned} \tag{2}$$

Se verifica sin duda que en todo sistema de valores de variables libres $x_{r+1}, \ldots, x_n$ del sistema (2) solo corresponde a una y solamente una solución del sistema (2) y, que parte, del sistema (1). En particular al sistema de valores nulos $x_{r+1} = 0, \ldots, x_n = 0$ solamente corresponde la solución nula del sistema (2) y del sistema (1).

Dese en el sistema (2) en una de las variables libres el valor igual a 1, mientras que las variables restantes serán consideradas como nulas. Se obtiene así $n-r$ soluciones del sistema de ecuaciones (2) que se denotara bajo la forma de filas en la matriz C:

$$C=\begin{bmatrix}\gamma_{11}\ \gamma_{21}\cdots\gamma_{r1} & 1\ 0\ \ldots 0\\ \gamma_{12}\quad\gamma_{22}\cdots\gamma_{r2} & 0\ 1\ \ldots\ 0\\ \quad\ldots\ldots\ldots\ldots\ldots & \\ \gamma_{1n-r}\ \gamma_{2n-r}\cdots\gamma_{r.n-r} & 0\ 0\ \ldots 1\end{bmatrix}$$

El sistemas de filas $C_{1\ ,\ \ldots,}\ C_{n-r}$de esta matriz es linealmente independientes. De hecho, para todos los escalares $\lambda_{1,\ \ldots,}\lambda_{n-r}$ en la igualdad

$$\lambda_1 C_{1\ +\ \ldots+}\ \lambda_{n-r}C_{n-r}\ =(0{,}0,\ \ldots,0)$$

Se deduce la igualdad

$$(\ldots,\lambda_1,\lambda_2,\ \ldots,\ \lambda_{n-r})=(0\ ,0\ ,\ \ldots,\ 0\ )$$

Y que parte, las igualdades

$$\lambda_1\ =0\,,\lambda_2=0,\ \ldots,\lambda_{n-r}=0.$$

Demuéstrese que la envoltura lineal del sistema de filas en la matriz C coincide con el conjunto de todas las soluciones del sistema (1). Sea

$$\mathbf{a}=(\boldsymbol{\alpha}_1,\ \ldots,\alpha_{\mathrm{r}}\ ,\alpha_{r+1}\,,\ \ldots,\alpha_n)$$

Una solución cualquiera del sistema (1).El vector

$$(\mathbf{d}=\mathbf{a}-(\alpha_{r+1}C_1+\alpha_{r+2}C_2\ +\ \ldots\ +\ \alpha_n C_{n-r})$$

Entonces es así una solución del sistema (1), además,

$$\mathbf{d}=(\delta_1\ ,\ \ldots,\delta_r\,,0,0\,,\ \ldots,0);$$

esta solución corresponde a los valores nulos de las variables libres $x_{r+1\ ,\ \ldots,}x_n$.Es decir $\mathbf{d}$es una solución nula del sistema (2) y del sistema (1); por lo tanto,

$$\mathbf{a}\ =\alpha_{r+1}C_1\ +\ \ldots\ +\alpha_n C_{n-r}\ \in L\ (C_1\,,\ \ldots,C_{n-r}).$$

En resumen se demostró que el conjunto de todas las soluciones del sistema (1) coincide con la envoltura lineal del sistema de vectores $C_1\ ,\ \ldots,C_{n-r}$. Por lo tanto, ese sistema de $n-r$ vectores es el sistema fundamental de soluciones por el sistema de ecuaciones (1).

Corolario 3.13 *Sea* $\boldsymbol{d}$*una solución del sistema no homogéneo de ecuaciones lineales (en el cuerpo*$\mathcal{F}$)

$$(I)\ \ \alpha_{i1}x_1\ +\ \ldots+\alpha_{in}x_n\ =\beta_i\qquad(i=1\ ,\ \ldots,\ m).$$

Y $C_1\,,\ \ldots,C_{n-r}$*el sistema fundamental de soluciones del sistema homogéneo de ecuaciones*

$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m).$

El conjunto

$$\{\mathbf{d} + \lambda_1 C_1 + \ldots + \lambda_{n-r} C_{n-r} \mid \lambda_1, \lambda_2, \ldots, \lambda_{n-r} \in \mathrm{F}\}$$

Entonces es el conjunto de todas las soluciones del sistema $(\boldsymbol{I})$.

Resolución del sistema de ecuaciones lineales por el método de eliminación sucesivo de variables . Dados los sistemas de ecuaciones lineales (en el cuerpo $\mathcal{F}$)

$\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1,$

(1) . . . . . .

$\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m.$

Plantéese

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}, \; B = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n}\beta_1 \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn}\beta_m \end{bmatrix}.$$

La matriz A se llama *matriz fundamental del sistema* (1), la matriz B *matriz completa del sistema* (1).

Un sistema de ecuaciones lineales se llama en escalar si la matriz completa del sistema es una matriz escalar sin filas con elementos para todos nulos .Un sistema de ecuaciones lineales se llama sistema reducida por escalones si la matriz completa del sistema es una matriz reducida por escalones.

Si B es una matriz nula, entonces todo vector en n dimensiones de F^{n}es una solución del sistema (1). Pero si A es una matriz nula, mientras que B no lo es, el sistema de ecuaciones (1) es entonces incompatible.

Supóngase que la matriz A no es nula. Entonces se puede reducir el sistema de ecuaciones (1) en un sistema escalar por las transformaciones elementales y en seguida, a un sistema reducido por escalones, siendo estos sistemas equivalentes al sistema inicial (1) Supóngase que las columnas $A^1, \ldots, A^r$ constituyen la base del sistema en las columnas de la matriz A. Mediante una serie de transformaciones elementales reduzcamos el sistema de ecuaciones (1)en un sistema escalar sin filas con elementos para todos nulos .Si esta ecuación anterior del sistema escalar obtenida es de la forma

$0.x_1 + \ldots + 0.x_n = \beta$, donde $\beta \neq 0$,

El sistema de ecuaciones en escalar obtenido es entonces incompatible y por lo tanto, es incompatible al sistema de ecuaciones (1) de partida que le es equipotente. Pero si dentro del primer miembro de la ecuación anterior del sistema escalar obtenido, hay coeficientes diferentes de cero, entonces el sistema en escalar obtenido toma la forma

$$\begin{aligned} \alpha'_{11}x_1 + \alpha'_{12}x_2 + \ldots + \alpha'_{1r}x_r + \ldots + \alpha'_{1n}x_n &= \beta'_1, \\ \alpha'_{22}x_2 + \ldots + \alpha'_{2r}x_r + \ldots + \alpha'_{2n}x_n &= \beta'_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \alpha'_{rr}x_r + \ldots + \alpha'_{rn}x_n &= \beta'_r, \end{aligned} \qquad (2)$$

Donde los coeficientes $\alpha'_{11}, \alpha'_{22}, \ldots, \alpha'_{rr}$ son diferentes de cero. El sistema (2) es compatible y equipotente al sistema inicial (1).

A partir del sistema escalar (2) pásese por una serie de transformaciones elementales al sistema de ecuaciones en escalar.

$$
\begin{aligned}
&x_1 \quad -\gamma_{1r+1}x_{r+1} - \ldots - \gamma_{1n}x_n = \delta_1,\\
(3)\quad &x_2 \quad -\gamma_{2r+1}x_{r+1} - \ldots - \gamma_{2n}x_n = \delta_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_r - \gamma_{rr+1}x_{r+1} - \ldots - \gamma_{rn}x_n = \delta_r.
\end{aligned}
$$

El sistema (3) es compatible y equipotente al sistema de ecuaciones (1) inicial. Si además $r = n =$, el sistema de ecuaciones (3) y el sistema (1) admite entonces una solución única (δ_1, δ_2 , $\ldots$, δ_n). Pero si $r(A) = r(B) < n$, el sistema (3) entonces es equivalente al sistema

$$
\begin{aligned}
&x_1 = \gamma_{1r+1}x_{r+1} + \ldots + \gamma_{1n}x_n + \delta_1,\\
(4)\quad &x_2 = \gamma_{2r+1}x_{r+1} + \ldots + \gamma_{2n}x_n + \delta_2\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_r = \gamma_{rr+1}x_{r+1} + \ldots + \gamma_{rn}x_n + \delta_r.
\end{aligned}
$$

Las ecuaciones del sistema (4) proporcionan una expresión explicita de las variable x_1 , $\ldots$, x_r llamadas principales a través de las variables x_{r+1} , $\ldots$, x_n llamadas libres. Atribuyendo en las ecuaciones (4) a las variables libres los valores cualquiera del cuerpo de escalares, se obtienen los valores correspondientes a las variables principales. Estamos así en capacidad de obtener cualquier solución particular del sistema de ecuación inicial (1), ya que es equipotente al sistema (4). Es por eso que, el vector

(5) $(\gamma_{1r+1}x_{r+1} + \ldots + \gamma_{1n}x_n + \delta_1, \ldots, \gamma_{rr+1}x_{r+1} + \ldots + \gamma_{1n}x_n + \delta_r, x_{r+1}, \ldots, x_n)$

Se llama *solución general del sistema de ecuaciones* (1).El vector (5) puede ser escrito bajo la forma de

(6) $x_{r+1}C_{r+1} + \ldots + x_nC_n + \delta$,

Donde C_{r+1} , $\ldots$, $C_n \in \mathrm{F}^n$ y $\delta = (\delta_1, \ldots, \delta_r, 0, \ldots, 0)$es la solución particular del sistema (1).El vector (6) es igualmente llamado *solución general del sistema* (1) se ve fácilmente que los vectores C_{r+1} , $\ldots C_n$ constituyen el sistema fundamental de soluciones de un sistema homogéneo de ecuaciones asociado al sistema (1).

El conjunto $\{x_{r+1}C_{r+1} + \ldots + x_nC_n + \delta | x_{r+1}, \ldots, x_n \in \mathrm{F}\}$es el conjunto de todas las soluciones del sistema de ecuaciones (1).

Para estudiar la compatibilidad del sistema dado de ecuaciones lineales (1) es necesario reducir la matriz completa B del sistema por una serie de transformaciones elementales en las filas en una matriz escalar B'. El sistema de ecuaciones lineales (1') en matriz completa B' es equipotente al sistema de ecuación inicial (1). El sistema de ecuaciones $(1')$ es incompatible si y solo si el rango de las filas de su matriz fundamental A' es inferior al rango de filas de la matriz completa B', es decir si en la última fila de la matriz en escalar B' todos los elementos a parte del anterior son nulos.

Ejercicios

1. Demostrar que una matriz no nula es equivalente por fila a una y solamente una matriz en escala reducida.

2. Demostrar que la matriz A de orden $m \times n$ es equivalente por fila a una matriz identidad de orden $n \times n$ si y solo si el rango de la matriz A vale n .

3. Mostrar que dos sistemas homogéneos lineales en el cuerpo $\mathcal{F}$ en variables x_1, $\ldots$, x_n son equivalentes si y solo si las matrices de sus sistemas son equivalentes por filas.

4. Sea $\mathcal{F}$ un cuerpo finito compuesto de K elementos. Mostrar que un sistema homogéneo dado de ecuaciones lineales en el cuerpo $\mathcal{F}$ en n variables posee k^{n-r} soluciones donde r es el rango de la matriz del sistema dado de ecuaciones.

5. Demostrar que un sistema compatible de ecuaciones lineales en matrices fundamentales no nulas solamente es equipotente a un solo y único sistema en escala reducida de ecuaciones lineales.

6. Demostrar que si dos sistemas compatibles de ecuaciones lineales son equipotentes, entonces los sistemas homogéneos de ecuaciones lineales que le son asociados son igualmente equipotentes.

7.Demostrar que dos sistemas compatibles de ecuaciones lineales en el cuerpo $\mathcal{F}$ en variables x_1 , . . . , x_n son equipotentes si y solo si las matrices completas de los sistemas son equivalentes por filas.

CAPITULO VI
MATRICES Y DETERMINANTES

§1. Operación sobre matrices y sus propiedades

Operación sobre matrices . Para todo este capitulo $\mathcal{F} = \langle \mathcal{F}, +, -, \ , 1\rangle$es un cuerpo de elección fija que llamaremos *cuerpos escalares.*

Los elementos del conjunto F serán llamados escalares.

Siendo $m\ y\ n$ los enteros positivos. El cuadro

$$A = \begin{bmatrix} \alpha_{11}\,\alpha_{12}\,.\,.\,.\,\alpha_{1n} \\ \alpha_{21}\ \alpha_{22}\ .\,.\,.\,\alpha_{2n} \\ .\ .\ .\ .\ .\ .\ .\ .\ . \\ \alpha_{m1}\ \alpha_{m2}.\,.\,.\,\alpha_{mn} \end{bmatrix}$$

En elemento de F se llama *matriz en el cuerpo* $\mathcal{F}$ o *matrizm* $\times\ n$ en $\mathcal{F}$;se denota brevemente $\| \alpha_{iK} \|$ y se le escribe $A = \| \alpha_{iK} \|$.Si $m = n$ la matriz A es una *matriz cuadrada de orden* n. El conjunto de todas las matrices $m \times n$ en el cuerpo $\mathcal{F}$ se denota $\mathrm{F}^{m\times n}$. En particular, el conjunto de todas las matrices cuadradas de orden n en $\mathcal{F}$ se denota $\mathrm{F}^{n\times n}$.

Consérvese las notaciones anteriores para las filas y columnas de la matriz A: la $i-$ ésima fila de la matriz A se denotaA_i :

$$A_i = [\alpha_{i1}, \alpha_{i2}, \ . \ . \ . \ , \alpha_{in}\,];$$

La k-esima columna se denotaA^K:

$$A^K = \begin{bmatrix} \alpha_{1K} \\ \alpha_{2K} \\ \vdots \\ \alpha_{nK} \end{bmatrix}$$

Dos matrices $m \times n\ A = \| \alpha_{iK} \|$ y $B = \| \beta_{iK} \|$son llamadas iguales y se escribe $A = B$ si $\alpha_{iK=}\beta_{iK=}$ para todos los índices $k\ e\ i$.

Una matriz se llama nula y se denota 0 si todos sus elementos son nulos.

Se llama suma de dos matrices $m \times n\ A\ y\ B$ la matriz $m \times n$ cuyo elemento ik-esimo es igual a $\alpha_{iK} + \beta_{iK}$, es decir

$$A + B = \| \alpha_{iK} + \beta_{iK} \|.$$

Se llama *producto escalar* λ *por la matriz* $A = \| \alpha_{iK} \|$ la matriz $m \times n$ $\| \lambda\alpha_{iK} \|$ denotada λA:

$$\lambda A = \| \lambda\alpha_{iK} \|.$$

Para la matriz $(-1)A$ se tiene la igualdad

$$A + (-1)A = 0.$$

Así la matriz $(-1)A$ es también denotada $-A$ y se llama *matriz opuesta a la matriz* A.

Sea $A \in \mathrm{F}^{m\times n}$Y $B \in \mathrm{F}^{n\times p}$:

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{\mathbf{11}} & \dots & \boldsymbol{\alpha_{1n}} \\ . \ . \ . \ . \ . \ . \ . \\ \boldsymbol{\alpha_{m1}} \dots & & \boldsymbol{\alpha_{mn}} \end{bmatrix},\ \boldsymbol{B} = \begin{bmatrix} \beta_{\mathbf{11}} & \dots & \boldsymbol{\beta_{1p}} \\ . \ . \ . \ . \ . \ . \ . \\ \boldsymbol{\beta_{n1}} \dots & & \boldsymbol{\beta_{np}} \end{bmatrix}$$

Se admite por lo tanto que el número de columnas de la matriz A es igual al número de filas de la matriz B.*El producto de la fila* A_i *por la columna* $B^{\mathcal{R}}$ se define así:

$$A_i B^k = [\alpha_{i1}, \ldots, \alpha_{in}] \begin{bmatrix} \beta_{1k} \\ \vdots \\ \beta_{nk} \end{bmatrix} =$$

$$= \alpha_{i1}\beta_{1k} + \ldots + \alpha_{in}\beta_{nk} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk}$$

Se llama *producto de matrices* $A\ Y\ B$ la matrice $m \times p$, cuyo elemento ik-esimo es igual en $A_i B^{\mathcal{R}}$, es decir

$$A.B = \begin{bmatrix} A_1B^1 & A_1B^2 \ldots A_1B^p \\ A_2B^1 & A_2B^2 \ldots A_2B^p \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ A_mB^1 & A_mB^2 \ldots A_mB^p \end{bmatrix}$$

En resumen, si A es la matriz $m \times n$ y B la matriz $n \times p$, entonces AB es la matriz $m \times p$.

TEOREMA 1.1.*Una multiplicación de matrices es asociativa, es decir para todas las matrices* $A, B\ Y\ C\ A(BC) = (AB)C$ si los productos AB y BC existen.

Demostración. Por hipótesis los productos AB y BC existen. Entonces se puede considerar que $A \in \mathrm{F}^{m\times n}$, $B \in \mathrm{F}^{n\times p}$, $C \in \mathrm{F}^{p\times q}$. Por lo tanto los productos $A(BC)$Y$(AB)C$ existen y pertenecen al conjunto $\mathrm{F}^{m\times q}$.Siendo $H = A(BC), H' = (AB)C$ y $h_{ik}h'_{ik}$ los ik-esimos elementos de las matrices H y H'respectivamente.
Demuéstrese que $h_{ik=}h'_{ik}$ para todos los índices $k\ e\ i$. De hecho,

$$\boldsymbol{h_{ik} = A_i(BC)^k = [\alpha_{i1}, \ldots, \alpha_{in}] \begin{bmatrix} B_1C^k \\ \vdots \\ \beta_nC^k \end{bmatrix} =}$$

$$\boldsymbol{= \alpha_{i1}B_1C^k + \ldots + \alpha_{in}B_nC^k =}$$

$$\boldsymbol{= \alpha_{i1}\sum_{s=p}^{p} \beta_{1s}\gamma_{sk} + \ldots + \alpha_{in}\sum_{s=1}^{p} \beta_{ns}\gamma_{sk} =}$$

$$\boldsymbol{= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk};}$$

$$\boldsymbol{h'_{ik} = (AB)_iC^k = \left[A_iB^1, \ldots, A_iB^p\right] \begin{bmatrix} \gamma_{1k} \\ \vdots \\ \gamma_{pk} \end{bmatrix} =}$$

$$\boldsymbol{= A_iB^1\gamma_{1k} + \ldots A_iB^p\gamma_{pk} =}$$

$$\boldsymbol{= (\sum_{j=1}^{n} \alpha_{ij}\beta_{j1})\gamma_{1k} + \ldots + (\sum_{j=1}^{n} \alpha_{ij}\beta_{jp})\,\gamma_{pk} =}$$

$$\boldsymbol{= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk};}$$

Por lo tanto $h_{ik=}h'_{ik}$ para todos los índices $k\ e\ i$, es decir $A(BC)$=$(AB)C$.□

TEOREMA 1.2. *Las operaciones con matrices están dotadas de las propiedades siguientes:*

(1) *El algebra* $\langle \mathrm{F}^{m\times n}, +, - \rangle$ *es un grupo abeliano*;

(2) $\alpha(A+B)=\alpha A+\alpha B$ $(\alpha,\beta\in \mathrm{F}, A, B\in \mathrm{F}^{m\times n})$;

(3) $(\alpha+\beta)A=\alpha A+\beta A$;

(4) $(\alpha\beta)A=\alpha(\beta A)$;

(5) $1.A=A$;

(6) *La multiplicación de las matrices es asociativa;*

(7) *La multiplicación de las matrices es distributivas en relación a la adición, es decir* $A(B+C)=AB+AC$ *si el producto* AB *y la suma* $B+C$ *existen; y* $(B+C)A=BA+CA$ *si el producto* BA *y la suma* $B+C$ *existen*;

(8) *Para todo escalar* λ *y todas las matrices* A, B *se tiene* $\lambda(AB)=(\lambda A)B=A(\lambda B)$ *Si el producto* AB *existe*.

Demostración. Las propiedades (1)-(5) se demuestran de la misma forma que las propiedades correspondientes a la adición de vectores y a la multiplicación por un escalar en los vectores de los espacios vectoriales aritméticos .

Según el TEOREMA 1.1 la multiplicación de las matrices es asociativa.

Demuéstrese que la multiplicación de las matrices es distributiva en relación a la adición. Sea $A\in \mathrm{F}^{m\times n}, B,\in C\ \mathrm{F}^{n\times p}$. Se verifica sin duda que $AB, AC\in \mathrm{F}^{m\times p}, B+C\in \mathrm{F}^{n\times p}$. De donde se deduce $A(B+C)\ y\ AB+AC$ son matrices $-m\times p$. Muéstrese que los $ik-$esimos elementos de esas matrices son iguales, es decir que $A_i(B+C)^{\mathcal{R}}=A_iB^{\mathcal{R}}+A_iC^{\mathcal{R}}$. De hecho,

$$A_i(B+C)^k=\sum_{j=1,..,n}\alpha_{ij}\left(\beta_{jk}+\gamma_{jk}\right);$$

$$A_i\beta^k+A_iC^k=\sum_{j=1,\dots,n}\alpha_{ij}\beta_{jk}+\sum_{j=1,\dots,n}\alpha_{ij}\gamma_{jk}=$$

$$=\sum_{j=1,\dots,n}\alpha_{ij}(\beta_{jk}+\gamma_{jk})$$

Por lo tanto, $A(B+C)=AB+BC$. Se demuestra de manera análoga que $(B+C)A=BA+CA$ si el producto BA y la suma $B+C$ existen.

Para demostrar la propiedad (8) búsquese los $ik-$ esimos elementos de las matrices $\lambda(AB), (\lambda A)B,\ A(\lambda B)$:

$$\lambda\left(A_iB^k\right)=\lambda\sum_{j=1}^{n}\alpha_{ij}\beta_{jk};\qquad (\lambda A_i)B^k=\sum_{j=1}^{n}(\lambda\alpha_{ij})\beta_{jk}$$

$$A_i\left(\lambda B^k\right)=\sum_{j=1}^{n}\alpha_{ij}(\lambda\beta_{jk})\ .$$

Estas tres expresiones son iguales entre ellas conforme a las propiedades de la adición y de la multiplicación de los escalares .Por lo tanto, $\lambda(AB)=(\lambda A)B=A(\lambda B)$.

Transposición del producto de las matrices . Sea $A=\|\ \alpha_{ik}\ \|$ la matriz $m\times n$ en el cuerpo $\mathcal{F}$. Se llama entonces, matriz transpuesta de A , la matriz $n\times m\ \|\ \beta_{ik}\ \|$ tal que $\beta_{ik}=\ \alpha_{ik}$ y se denota ${}^{\mathrm{t}}A$.

Por lo tanto se obtiene la matriz transpuesta intercambiando las filas y las columnas de la matriz dada. En particular,

$$({}^{\mathrm{t}}A)^i={}^{\mathrm{t}}[\alpha_{i1},\ldots\alpha_{in}]=\begin{bmatrix}\alpha_{i1}\\ \vdots\\ \alpha_{in}\end{bmatrix};$$

$$({}^{\mathrm{t}}A)_k=\begin{bmatrix}\alpha_{ik}\\ \vdots\\ \alpha_{mk}\end{bmatrix}=[\alpha_{ik},\ldots\alpha_{mk}].$$

TEOREMA 1.3. *Si el producto AB de las matrices$A\ y\ B$ existe, también existe un producto*${}^{t}B.{}^{t}A\ y\ {}^{t}(AB) = {}^{t}B.{}^{t}A.$

Demostración. Supóngase que $A \in \mathrm{F}^{m\times n}$, $B \in \mathrm{F}^{n\times p}$.Entonces si $C = AB, AB \in \mathrm{F}^{m\times p}\ y\ {}^{t}(AB) \in \mathrm{F}^{p\times m.}$Además${}^{t}B \in \mathrm{F}^{p\times n} y\ {}^{t}A \in \mathrm{F}^{p\times n}$ .Por lo tanto, el producto${}^{t}B.{}^{t}A$ existe y ${}^{t}B{}^{t}A \in \mathrm{F}^{p\times m}$.Las matrices $C = {}^{t}(AB) y\ C' = {}^{t}B.{}^{t}A$ son asi las matrices $p \times m$.Verifiquese que los ik −esimos elementos $C_{i\mathcal{R}}\ y\ C'_{i\mathcal{R}}$ de esas matrices son iguales .De hecho,

$$C_{ik} = A_k B^i = [\alpha_{k1},\ldots\alpha_{kn}]\begin{bmatrix}\beta_{1i}\\ \vdots \\ \beta_{ni}\end{bmatrix} = \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni}\ ;$$

Por otra parte

$$C'_{ik} = ({}^{t}B)_i({}^{t}A)^k = [\beta_{1i}\ ,\quad \ldots \quad ,\beta_{ni}]\begin{bmatrix}\alpha_{k1}\\ \vdots \\ \alpha_{kn}\end{bmatrix} =$$

$$= \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni}\ .$$

Por lo tanto $C_{ik} = C'_{ik}$ para todos los índices $k\ e\ i$ es decir ${}^{t}(AB) == {}^{t}B.{}^{t}A.$ □

Ejercicios

1. Sea $A = \begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}$. Buscar A^n para todo entero positivo n.

2. Demostrar que si para la matriz $A\ y\ B$ los productos $AB\ y\ BA$ existen y$AB = BA$, las matrices $A\ y\ B$ son cuadradas y poseen un mismo orden.

3. Sea $A\ y\ B$ las matrices cuadradas del mismo orden y $AB = BA$.Demostrar que para todo entero positivo n es verdadera la formula

$$(A+B)^n = A^n + n.A^{n-1}.B + \frac{n(n-1}{2}A^{n-2.}B^2 + \ldots + B^n.$$

4. Mostrar que la operación de transposición está dotada de las propiedades siguientes (a)${}^{t}(A+B) = {}^{t}A + {}^{t}B;\quad (b)\quad {}^{t}(\lambda A) = \lambda.{}^{t}A$, donde λ es un escalar ;(c)${}^{t}(A^{-1}) = ({}^{t}A)^{-1}; (d)\quad {}^{t}(ABC) = {}^{t}C.{}^{t}B.{}^{t}A$ si el producto ABCexiste.

5. Una matriz cuadrada A se llama *simétrica* si $A = {}^{t}A$.Mostrar que si A es una matriz cuadrada, la matriz $A + {}^{t}A$ es simétrica.

6. Una matriz cuadrada A se define *simétrica a la izquierda* si $A = -{}^{t}A$.Demostrar que toda matriz cuadrada se puede representar y de esa manera única, bajo la forma de suma de matrices simétricas y simétricas a la izquierda.

7. Demostrar que las transformaciones elementales en las columnas de una matriz pueden ser realizadas en medio de una multiplicación en la matriz a la derecha por las matrices elementales correspondientes.

§2. Matrices inversibles

Matrices inversibles. Sea Auna matriz $n \times n$ en el cuerpo de escalares $\mathcal{F}$.Si E es una matriz identidad $n \times n$ entonces tenemos

(1) $\quad AE = A = EA.$

Una matriz cuadrada se define invertible si existe una matriz B que cumple las condiciones

(2) $\quad AB = E,\ \ BA = E.$

La matriz B que satisface a esas condiciones se define inversa de A.

Las matrices $A\ y\ B$ se llaman mutualmente inversas.

PROPOSICION2.1. Si la matriz A es inversible, entonces no existe solo una matriz inversa de A.

Demostración. Supóngase que $B\ y\ C$ son las matrices inversas de A. Entonces tenemos $AC = E = BA\ y\ B = BE = B(AC) = (BA)C = E.C = C$, es decir que $B = C.$ □

Si la matriz A es inversible, entonces la matriz inversa de A se denota A^{-1}. Por lo tanto, para toda matriz inversible tenemos las igualdades

(3) $AA^{-1} = E, \qquad A^{-1}A = E$

El conjunto de todas las matrices invertibles $n \times n$ en el cuerpo $\mathcal{F}$ se denota $GL(n, \mathcal{F})$.

TEOREMA 2.2.El álgebra $\langle GL(n, \mathcal{F}), \ . \ , -1)$ es un grupo.

Demostración .L a matriz unidad E es evidentemente, invertible y en razón de (1), es un elemento neutro.

Si la matriz A es inversible, entonces en virtud de (2) la matriz A^{-1} es igualmente inversibles.

El conjunto $GL(n, \mathcal{F})$ de las matrices inversibles $n \times n$ es igualmente cerrado en relación a la multiplicación. De hecho si $A, B \in GL(n, \mathcal{F})$, entonces se tiene

$$(AB)(B^{-1}A^{-1}) = E = (B^{-1}A^{-1})(AB)$$

Es decir que la matriz AB es inversible en $\mathcal{F}$ y por tanto corresponde al conjunto $GL(n, \mathcal{F})$.

En fin según el TEOREMA 1.1, la multiplicación de las matrices es asociativa.□

COROLARIO 2.3. *Un producto arbitrario de las matrices invertibles es una matriz invertible.*

Matrices elementales . Introdúzcase la noción de matriz elemental.

DEFINICIÓN. La matriz cuadrada obtenida a partir de la matriz identidad por transformación elemental regular en las filas (las columnas) se llama matriz elemental asociada a esta transformación .

Es así que están las matrices elementales de segundo orden las matrices

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}, \begin{bmatrix}\lambda & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & \lambda\end{bmatrix}, \begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}$$

Donde λ es un escalar no nulo cualquiera.

La matriz elemental se obtiene a partir de una matriz identidad E por una de las transformaciones regulares siguientes:

1. La multiplicación de la fila (de la columna) de la matriz Epor un escalar diferente de cero;
2. La adición (sustracción) en una fila (o columna) cualquiera de la matriz E de una otra fila (columna) multiplicada por un escalar.

Desígnese para $E_{\lambda(i)}$la matriz obtenida a partir de la matriz E después de lmultiplicación de la i-esima fila por un escalar λ no nulo:

$$E_{\lambda(i)} = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Desígnese para $E_{(i)+\lambda(k)}(E_{(i)-\lambda(k)})$ la matriz obtenida a partir de la matriz E despues de la adición (sustracción) en la i −esima fila de la k -esima fila multiplicada por λ:

$$E_{(i)+\lambda(k)} = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} \qquad E_{(i)-\lambda(k)} = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & -\lambda & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Se escribirá E_φ la matriz obtenida apartir de la matriz identidad E después de la aplicación en la transformación elemental φ en las filas; asíE_φ es la matriz correspondiente a ala transformación φ .

Considérese algunas propiedades de las matrices elementales.

PROPIEDAD 2.1*. Toda matriz elemental es invertible .Una matriz inversa de la matriz elemental es una matriz elemental.*

Demostración. Una verificación directa muestra que para todo escalar λ diferente de cero y $k\ e\ i$ cualquiera se tiene las igualdades.

$E_{\lambda(i)}E_{\lambda-1(i)} = E = E_{\lambda-1(i)}$;

$E_{(i)+\lambda(k)}E_{(i)-\lambda(k)} = E = E_{(i)-\lambda(k)}E_{(i)+\lambda(k)}$.

En la base de esas igualdades se concluye que tenemos la propiedad 2.1.□

PROPIEDAD2.2 Un producto de matrices elementales es una matriz invertible.

Esta Propiedad se basa directamente en la propiedad 2.1 y en el corolario 2.3

PROPIEDAD 2.3. *Si una transformación elemental regular por filas φ Coloca la matriz $m \times n\ A$ en la matriz B, tenemos entonces $B = E_\varphi A\left(E_\varphi \in \Gamma^{m\times m}\right)$. La reciproca es igualmente verdadero*.

Demostración .Si φ es una multiplicación de la $i - esima$ fila $A = \| \alpha_{ik} \|$ por un escalar no nulo λ, se tiene

$$E_{\lambda(i)}A = \begin{bmatrix} \alpha_{11} \ . \ . \ . \alpha_{1n} \\ . \ . \ . \ . \ . \ . \ . \ . \ . \\ \lambda\alpha_{i1} \ . \ . \ . \lambda\alpha_{1n} \\ . \ . \ . \ . \ . \ . \ . \ . \ . \\ \alpha_{m1} \ . \ . \ . \alpha_{mn} \end{bmatrix}$$

Es decir $B = E_\varphi A$. Pero si $E_\varphi = E_{(i)+\lambda(k)}$, entonces

$$E_{(1)} + \lambda_{(k)}\ A = \begin{bmatrix} \alpha_{11} & . \ . \ . \alpha_{1n} \\ . \\ \alpha_{i1} + \lambda\alpha_{k1} & . \ . \ . \ \alpha_{in} + \lambda\alpha_{kn} \\ . \\ \alpha_{m1} & . \ . \ . \alpha_{mn} \end{bmatrix}$$

Es decir $B = E_{(i)+\lambda(k)}.A$.

Se verifica sin duda que la afirmación inversa es igualmente verdadera.

PROPIEDAD 2.*4 Si la matriz C se obtiene a partir de la matriz A por una serie de transformaciones elementales regulares por fila $\varphi_1,\ . \ . \ . ,\ \varphi_s$, entonces tenemos $C = E_\varphi\ . \ . \ . E_\varphi.A$ .La reciproca es igualmente verdadera*.

Demostración .Según la propiedad 2.3 la transformación $\varphi_1$convierte la matriz A en la matriz $E\varphi_1.A$, $\varphi_2$convierte la matriz $E\varphi_{s-1}.\ .\ .E\varphi_1.A$ en la matriz $E\varphi_s E\varphi_{s-1}.\ .\ .E\varphi_1.A$.

Por lo tanto $C = E\varphi_s.\ .\ .E\varphi_2 E\varphi_1.A$.

Se verifica fácilmente que la reciproca es igualmente verdadera

Condición de inversibilidad de la matriz. Para demostrar el TEOREMA 2.8 necesitamos de tres lemas siguientes.

LEMA2.4.*Una matriz cuadrada en fila (columna) cuyos elementos son nulos e irreversibles.*

Demostración .Sea A una matriz cuadrada cuya fila está en elementos nulos, siendo B una matriz cualquiera $A, B \in \Gamma^{n\times n}$.

Sea $A_i$la fila en elementos nulos de la matriz A, entonces se tiene

$(AB)_i = [A_iB^1, \dots, A_iB^n] = [0, \dots, 0]$,

Es decir que la $i - esima$ fila de AB posee solamente elementos nulos. Por tanto la matriz A es irreversible. □

LEMA 2.5 *Si las filas de una matriz cuadrada son linealmente dependientes, la matriz es entonces irreversible*.

Demostración .Sea A una matriz cuadrada en las filas linealmente dependientes .Existe entonces una serie de transformaciones elementales regulares por fila que hace pasar$A$ en una matriz escalar; sea$\varphi_1, \ldots, \varphi_s$ esta serie. Según la propiedad 2.4 las matrices elementales tienen la igualdad

(1)$E\varphi_s \ldots E\varphi_1 . A = C$,

Donde C es una matriz con filas en elementos para todos nulos. Por lo tanto, según el lema 2.4 la matriz C es irreversible .Pero si al contrario, la matriz A era inversible, el producto ala izquierda en la igualdad (1) sería entonces una matriz inversibles, como producto de matrices inversibles (ver corolario 2.3), lo que es imposible. Entonces la matriz A es irreversible.□

COROLARIO2.6. *Si una matriz cuadrada es invertible, sus líneas son entonces linealmente independientes.*

LEMA 2.7 *Una matriz cuadrada en filas linealmente independientes se puede representar bajo la forma de un producto de matrices elementales*.

Demostración. Sea A una matriz cuadrada en filas linealmente independientes. Existe una serie de transformaciones elementales regulares por filas $\varphi_1, \ldots, \varphi_s$ que hace pasar la matriz A en la matriz identidad E. Según la propiedad 2.4 de las matrices elementales, se deduce que $E\varphi_s, \ldots, E\varphi_1 . A = E$. Por lo tanto, $A = E_{\varphi S}^{-1} \ldots E_{\varphi 1}^{-1}$, donde según la propiedad 2.1 las matrices elementales, los factores $. E_{\varphi 1}^{-1}, \ldots E_{\varphi S}^{-1}$ Son las matrices elementales.□

TEOREMA 2.8 Para toda matriz cuadrada $A(A \in \mathrm{F}^{n\times n})$ las tres afirmaciones siguientes son equipotentes:

(a) La matriz A es inversible;

(b) Las filas (columnas) de la matriz A son linealmente independientes;

(c) La matriz A se puede representar bajo la forma de un producto de matrices elementales.

Demostración. Según el corolario del lema 2.5, (b) es secuencia de (a).Posteriormente, según el lema 2.7(c) es secuencia de (b).

Finalmente, conforme a la propiedad 2.2 de las matrices elementales y del corolario 2.3,(a) surge de (c).Por lo tanto, las afirmaciones (a),(b) y(c) son equipotentes.

Calculo de la matriz inversa. Ahora se está en capacidad de establecer una regla muy simple de cálculo de la matriz inversa.

TEOREMA 2.9 *Si por una serie de transformaciones elementales por filas se hace pasar una matriz cuadrada A en una matriz identidad E la matriz A. Entonces es inversible y de esta misma serie de trasformaciones que hace pasar la matriz E en la matriz A^{-1}.*

Demostración. Supóngase que $\varphi_1, \ldots, \varphi_s$ es la serie de transformaciones que hace pasar la matriz cuadrada A en la matriz identidad E. Entonces, según la propiedad 2.4 las matrices elementales,

$$E = E\varphi_s, \ldots, E\varphi_1 A.$$

Conforme a la proposición 2.1 se deduce que la matriz A es inversible y

$$A^{-1} = E\varphi_s \ldots E\varphi_1 E$$

Según la propiedad 2.4 de las matrices elementales, resulta de la última igualdad que la serie de transformaciones elementales por filas $\varphi_1, \ldots, \varphi_s$ transforma la matriz E en la matriz A^{-1}.□

El TEOREMA 2.9 Permite formular la regla siguiente de obtención de la matriz inversa. *Para encontrar la matriz inversa de la matriz A de orden $n \times n$, es necesario pasar la matriz rectangular $n \times 2n(A \setminus E)$ en una matriz de la forma $(E \setminus C)$ por una serie de transformaciones elementales regulares por filas; la matriz C obtenida de esta manera es inversa a la matriz A.*

Notación y resolución del sistema de n ecuaciones lineales en n variables bajo la forma matricial

.Considérese un sistema de ecuaciones lineales

$$(I)\quad \begin{aligned} &\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{n1}x_1+\ldots+\alpha_{nn}x_n=\beta_n \end{aligned}$$

En la estructura$\mathcal{F}$. Al introducir las notaciones

$$\boldsymbol{A}=\begin{bmatrix}\alpha_{11} & \ldots & \alpha_{1n}\\ \ldots & \ldots & \ldots\\ \alpha_{n1} & \ldots & \alpha_{nn}\end{bmatrix},\qquad \boldsymbol{b}=\begin{bmatrix}\beta_1\\ \vdots\\ \beta_n\end{bmatrix},\qquad \mathcal{X}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix},$$

Se está en capacidad de escribir el sistema (I) bajo la forma de una ecuación matricial

(2) $A\mathcal{X}=b.$

Se ve inmediatamente que la ecuación (2) es equipotente al sistema de ecuaciones (I).Se llama forma matricial de escritura del sistema de ecuaciones (I).

TEOREMA 2.10 *Si las filas de la matriz A son linealmente independientes, el vector$A^{-1}b$ entonces es la única solución de la ecuación (2).*

Demostración. Supóngase que un vector columna$\mathcal{X}_0$ es la solución de la ecuación (2) es decir que $A\mathcal{X}_0=b$. Al multiplicar a la izquierda los dos miembros de la igualdad $A\mathcal{X}_0=b$.por A^{-1} se obtiene

(3) $\mathcal{X}_0=A^{-1}.b.$

De este modo podría ser la ecuación (2) que posee una solución $A^{-1}b$ o no la posee. Sin embargo, la igualdad $A(A^{-1}.b)=b$ muestra que el vector $A^{-1}.b$ es una solución de la ecuación (2).Por lo tanto, el vector $A^{-1}.b$ es la única solución de la ecuación (2).□

COROLARIO 2.11. *Si las filas de la matriz fundamental A del sistema (I) son linealmente independientes, el sistema entonces es compatible y el vector $A^{-1}.b$ es la solución única de ese sistema.*

Ejercicios

1. Sea$A=\|\ \alpha_{ij}\ \|$ una matriz cuadrada de orden n(en el cuerpo$\mathcal{F}$).Nótese $E_{ik}(i,k=1,\ \ldots,n)$ la matriz cuya $i-$esima fila k-esima columna tienen 1 por elemento, los elementos restantes son nulos .Mostrar que

(*)$AE_{ik}=\alpha_{1i}E_{ik}+\ldots+\alpha_{ni}E_{nk}$,$E_{ik}A=\alpha_{k1}E_{i1}+\ldots+\alpha_{kn}E_{in}$.

2. En la base a la igualdad (*) demostrar que la matriz A es permutable con cada una de las matrices E_{ik} si y solo si A es de la forma λE,donde $\lambda\in$ F.

3. Utilizando el resultado del problema precedente mostrar que la matriz A es permutable con cualquier matriz cuadrada de orden n(en la estructura$\mathcal{F}$) si y solo si $A=\lambda E$,donde $\lambda\in$ F.

4. Sea A una matriz cuadrada de orden n .Demostrar que la matriz A es permutable con una matriz diagonal cualquiera de orden n si y solo si la matriz A es ella misma diagonal.

5. Sea$A$ una matriz diagonal, todos los elementos de la diagonal principal siendo diferentes el uno del otro .Mostrar que toda matriz es permutable con A es también diagonal.

6.Mostrar que una matriz cuadrada A de orden n es permutable con una matriz cualquiera simétrica del mismo orden es una matriz escalar ,es decir que $A=\lambda E$,donde λ es un escalar y E una matriz identidad de orden n .

7. Sea$A$ una matriz cuadrad de orden n(en la estructura$\mathcal{F}$).Demostrar que el conjunto de todas las matrices (en$\mathcal{F}$), permutables con la matriz A es cerrado en relación a la adicion y en relación a la multiplicación.

§ 3. Permutaciones

Permutación. Grupo de permutaciones. Considérese las permutaciones del conjunto $M = \{1, \ldots, n\}$, donde n es un número natural distinto de cero .Se llama permutación del conjunto M la función inyectiva del conjunto M sobre el mismo.

Toda función φ del conjunto M sobre el mismo se escribe de manera cómoda bajo la forma de tabla

$$\varphi = \begin{pmatrix} 1 & 2 \ldots n \\ \varphi(1) & \varphi(2) \ldots \varphi(n) \end{pmatrix}$$

El orden de los números de la primera fila tiene poca importancia y puede variar de cualquier manera .Sin embargo, es necesario asegurarse en que para todo k el numero $\varphi(k)$ sea remplazado inmediatamente debajo de k.

El conjunto de todas las permutaciones del conjunto M será escrito S_n; los elementos de este conjunto son llamados permutaciones de índice n.

si $\varphi \in S_n$, entonces (1) φ es una función inyectiva ,es decir que para todos $k\ e\ i \in M$ se deduce de $\varphi(i) = \varphi(k)$ que $i = k$; (2) φ es una función de M sobre la misma ,es decir $\{\varphi(1), \ldots, \varphi(n)\} = \{1, \ldots, n\}$. Siendo M un conjunto finito ,de la condición (1) se deduce la condición (2),y recíprocamente.

El producto $\varphi\psi$ de dos permutaciones φ y ψ del conjunto M se define como una composición de funciones φ y ψ ($\varphi\psi = \varphi.\psi$.

Por lo tanto, por definición, $\varphi\psi(i) = \varphi\left(\psi_{(i)}\right)$, $\quad i = 1, \ldots, n$.

Una composición de cada dos funciones inyectivas del conjunto M sobre si misma es una función inyectiva del conjunto M sobre sí mismo. Por lo tanto, para dos permutaciones cualquieras φ, ψ de S_n tenemos $\varphi\psi \in S_n$.

Nótese para ε la función idéntica del conjunto M sobre si mismo.

$\varepsilon(i) = i$, $\quad i = 1, \ldots, n$, es decir $\varepsilon = \begin{pmatrix} 1 & 2 \ldots n \\ 1 & 2 \ldots n \end{pmatrix}$.

Se constata fácilmente que para toda permutación φ de $S_n \varphi\varepsilon = \varepsilon\varphi = \varphi$, es decir que ε es un elemento neutro en relación a la multiplicación.

Si φ es una permutación del conjunto M, φ^{-1} es igualmente una permutación del conjunto M y $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$.Ademas

$$\varphi^{-1} = \begin{pmatrix} \varphi(1) & \ldots & \varphi(n) \\ 1 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & n \\ \varphi^{-1}(1) & \ldots & \varphi^{-1}(n) \end{pmatrix}$$

TEOREMA 3.1 El algebra $\langle S_n, \ , {}^{-}1\rangle$ es un grupo.

Demostración. Se estableció anteriormente que el conjunto S_n es cerrado a las operaciones principales. , $^{-1}$. Según el TEOREMA 2.3, una composición de funciones es asociativa. Una permutación idéntica ε es un elemnto neutro en relación a la multiplicación y, para cualquier permutación φ de S_n se tene la igualdad $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$. De este modo el algebra $\langle S_n, \ldots, {}^{-}1\rangle$ entonces es un grupo. □

DEFINICIÓN. El grupo $\langle S_n, \ , {}^{-}1\rangle$ se llama grupo simétrico de índice n y se denota $\mathcal{L}n$. El elemento ε se nombra elemento identidad de ese grupo.

Permutaciones pares e impares . Sea dada una permutación del conjunto $M = \{1, \ldots, n\}$

$$\varphi = \begin{pmatrix} 1 & 2 \ldots n \\ \varphi(1) & \varphi(2) \ldots \varphi(n) \end{pmatrix}.$$

Considérese un par no ordenado $\{i, k\}$ de elementos diferentes del conjunto M. El par $\{i, k\}$ se llama regular relativamente a la permutación φ si las diferencias $i - k\ y\ \varphi(i)\ y\ \varphi(i) - \varphi(k)$ son afectados del mismo signo .Se dice que el par $\{i, k\}$ es irregular relativamente a la permutación φ o y constituye una inversión si las diferencias $i -$

$k\ y\ \varphi(i)\ y\ \varphi(i) - \varphi(k)$cuentan con signos opuesto .Es así ,por ejemplo, que en la permutación idéntica $\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$ no hay inversión. En la permutación $\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$solamente tenemos una inversión.

En la permutación$\begin{pmatrix}1\ 2\ 3\\ 3\ 1\ 2\end{pmatrix}$n hay dos inversiones.

La permutación se llama par si esta lleva un número par de inversiones; esta se llama impar si el número de inversiones es impar. Es así, por ejemplo, que una permutación idéntica es par.

La permutación φ de la forma

$\begin{pmatrix}1 \dots i \dots\ k \dots n\\ 1 \dots\ k \dots i \dots\ \ n\end{pmatrix}$

se llama transposición. Dicho de otro modo, la permutación φse llama *transposición* si existe un par *{*i, *κ} de elementos diferentes de* M *que cumple con las condiciones*

$\varphi\ \ (i\ ) =, \kappa\varphi\ (\kappa)\ =\ i, \varphi\ (s)\ =\ s$

Para cada $s\ \epsilon\ M \setminus \{i, \kappa\}$.

LEMA 3.2. Toda transposición es una permutación impar.

Demostración. Seaφ una transposición que hace pasar $i$enκ(i $\neq \kappa$), es decir que cumple con las condiciones (1). Plantéese que i $< \kappa$. Se ve sin duda que el par {s, t} $\sqsubset M$ puede constituir una inversión si al menos uno de los elementos es i o κ; en el caso contrario las dos diferencias $S - t\ y\ \varphi\ (t)$ coinciden.

Si $i <\ S\ o\ \kappa <\ s$, no hay inversiones entre los pares $\{s, i\}\ y\ \{\kappa, s\}$ puesto que las dos diferencias son negativas.

Si $i < s \leq k$, entre los pares$\{i, s\}$ son inversiones los pares siguientes: $\{i, i\ +1\}, \cdots, \{i, k\}$, en total $k -$ i inversiones.

Si $i < s < k$, entre los pares $\{s, k\}$ son inversiones los pares$\{i + 1, k\}, \cdots, \{k - 1, k\}$; hay un total $k - i -$ 1inversiones.

En resumen, la transposición φconsta de un total $(\kappa{-}i) +\ (k - 1)\ =\ 2\ (-\kappa i) - i - 1$ inversiones, y, por consiguiente,φ es una permutación impar.

Signatura de una permutación. La signatura de cualquier número racional se define de la siguiente manera:

$$\text{Sing (a)} = \begin{cases} 1\ para\ a > 0, \\ 0\ para\ a\ = 0, \\ -1\ paraa < 0. \end{cases}$$

Se observa a continuación que *para cualquier número racional,*$a\ y\ b$ *se tiene*$sing(ab) = sing(a).sing(b)$.*Esta propiedad de la signatura se llama propiedad multiplicativa* y esta se utilizara para la demostración de lema 3.3.

Nótese sgn la función de un conjunto Sn en un conjunto$\{1, -1\}$definido por la igualdad:

$$\text{Sgn}\varphi = \begin{cases} 1, si\varphi es\ una\ permutacion\ par. \\ -1, si\ \varphi\ es\ una\ permutacion\ impar. \end{cases}$$

Se ve sin duda que la signatura (sgnφ) de la permutación φ es igual al producto de las signaturas de cualquier número $\frac{\text{i} - \kappa}{\varphi\ (\text{i}) - \varphi\ (\kappa)}$ correspondiente a todos los pares posibles$\{i, \kappa\}$ de diversos elementos del conjunto M, es decir que

$$sgn\varphi = \prod_{\substack{\{i,k\}\subset M \\ i\neq k}} sing\frac{i-k}{\varphi(i) - \varphi(k)}.$$

LEMA 3.3. *La signatura de un producto de dos permutaciones es el producto de signaturas de estas permutaciones, es decir*

$sgn(\varphi\psi) = sgn\varphi \cdot sgn\psi(\varphi, \psi\ \in\ S_n)$.

Demostración. Se puede representar la permutación

$\varphi = \begin{pmatrix} \psi(1) \dots \psi & (n) \\ \varphi\psi(1) \dots \varphi\psi & (n) \end{pmatrix}$; Entonces,

$$sgn\varphi = \prod_{\substack{\{i,k\}\subset M \\ i\neq k}} sign\frac{\psi(1)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)};$$

Como resultado, se obtiene

(2) $$sgn\varphi \cdot sgn\psi = \prod_{\substack{\{i,k\}\subset M \\ i\neq k}} sign\ \frac{\psi(1)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \times$$

$$\times \prod_{\substack{\{i,k\}\subset M \\ i\neq k}} sign\frac{i-k}{\psi(i)-\varphi\psi(k)\cdot}$$

Conforme a la propiedad multiplicativa de la signatura

$$\operatorname{sign}\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \cdot \operatorname{sign}\frac{i-k}{\psi(i)-\psi(k)} =$$

$$= \operatorname{sign}\left(\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \cdot \frac{i-k}{\psi(i)-\psi(k)}\right) = \operatorname{sign}\frac{i-k}{\varphi\psi(i)-\varphi\psi(k)\cdot}$$

También se deduce de (2) que

$$sgn\varphi.sgn\psi = \prod_{\substack{\{i,k\}\subset M \\ i\neq k}} sign\frac{i-k}{\varphi\psi(i)-\varphi\psi(k)} = sgn(\varphi\psi).\ \square$$

TEOREMA3.4. *La signatura de una permutación (función sgn) dotada de las siguientes propiedades:*
La función sgn es multiplicativa, es decir $sgn(\varphi\psi) =$

$= sgn\varphi \cdot sgn\psi paratodos\varphi, \psi\ de\ S_n;$

La signatura de la transposición vale (-1)*;*
Las permutaciones inversas entre ellas tienen una misma signatura;
Si τ *es una transposición y* φ *es una permutación cualquiera de* S_n*, entonces se tenemos sgn* $(\tau\varphi) = sgn(\varphi\tau) = -sgn\varphi$.

Demostración. La propiedad (1) se verifica a partir del lema 3.3. La propiedad (2) proviene directamente del lema 3.2. Conforme a la propiedad (1),

$sgn\ (\varphi\varphi^{-1}) = sgn\varphi \cdot sgn\varphi^{-1} = sgn\varepsilon = 1$

Para toda permutación φ. Como resultado, $sgn\varphi = sgn\varphi^{-1}$. La propiedad (4) proviene directamente de las propiedades (1) y (2). □

COROLARIO 3.5. *El producto de dos (o de un número par) de permutaciones de la misma paridad es una permutación par*.

COROLARIO 3.6. El producto de dos permutaciones de paridad diferente es una permutación impar.

Ejercicios

1. Demostrar que existe $n!$ permutaciones de un conjunto compuesto de n elementos.
2. Mostrar si $n > 1$ el número de permutaciones pares del conjunto $\{1,2,\cdots,n\}$ es igual al número de permutaciones impares.
3. Demostrar que el conjunto de todas las permutaciones pares de S_n es cerrado con respecto a la multiplicación y a la operaciónde obtención del inverso del elemento.
4. Mostrar que cada permutación de $S_n$para $n > 1$ puede representarse bajo la forma de un producto de transposición del aspecto $(k, k+1)$, donde $1 \leq k < n$.
5. Mostrar que cada permutación de S_n para $n > 1$ puede representarse bajo la forma de un producto de transposición del aspecto $(1, k)$, donde $1 < k \leq n$.

§4. Determinantes

Determinante de una matriz cuadrada. Sea$\mathcal{F}$un anillo conmutativo o un cuerpo cuyos elementos serán nombrados *escalares*. Sea

$$A = \begin{bmatrix} \alpha_{11}\,\alpha_{12}\cdots\alpha_{1n} \\ \alpha_{21}\alpha_{22}\ldots\alpha_{2n} \\ \cdots\cdots\cdots\cdots \\ \alpha_{n1}\alpha_{n2}\ldots\alpha_{nn} \end{bmatrix}$$

Una matriz en,$\mathcal{F}$, AF^{nxn}. Sea $S_n$el conjunto de todas las permutaciones del conjunto $\{1,\cdots n,\}$ ·

Considérese el conjunto $M(A)$ de cualquiera de los productos de elementos de la matriz$A$ tomados para una de cada fila y columna. Cualquier elemento del conjunto $M(A)$ consta de n factores y también se puede escribir:

$$a_{1i_1}.\,a_{2i_2}\ldots a_{ni_n}.$$

Hágase corresponder al elemento (1) la permutación

$$\begin{pmatrix} 1 & 2\cdots n \\ i_1 & i_2\cdots i_n \end{pmatrix}$$

del conjunto $\{1,\cdots,n\}$.Reciprocamente: a cada permutación τ de S_n,

$\tau = \begin{pmatrix} 1 & 2\cdots n \\ \tau(1) & \tau(2)\cdots\tau(n) \end{pmatrix}$,

Corresponde un elemento único de un conjunto $M\ (A)$, se obtiene

$$a_{1\tau(1)}.a_{2\tau(2)}\cdots a_{n\tau(n)}\ \cdot$$

Así mismo, la función asociada a cada permutación τ de $S_n$del elemento (4) de un conjunto $M(A)$ es *una función inyectiva* del conjunto S_n en $M(A)$ ·

DEFINICIÓN. Se llama determinante de la matriz$A$ la suma

$$\sum_{\tau\in Sn} sgn(\tau)\, a_{1\tau(1)}\cdot a_{2\tau(2)}\cdots a_{n\tau(n)}\ \cdot$$

La suma consta $n!$ Términos y a cada permutación τ de S_n en esta suma corresponde exactamente un término.

Se denotara el determinante de la matriz$A|A|$ o det A, o

$$\begin{vmatrix} \alpha_{11}\ \cdots\alpha_{1n} \\ \cdots\ \cdots \\ \alpha_{n1}\cdots\alpha_{nn} \end{vmatrix}.$$

Si $n = 1$, det $[\alpha_{11}] = \alpha_{11}$ · Para $n = 2$

$$\begin{vmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{vmatrix} = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}\,.$$

Si $n = 3,$ se tiene

$$\begin{vmatrix}\alpha_{11}\alpha_{12} & \alpha_{13}\\ \alpha_{21}\alpha_{22} & \alpha_{23}\\ \alpha_{31} & \alpha_{32}\alpha_{33}\end{vmatrix} = \alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{13}\alpha_{21}\alpha_{32} + \alpha_{12}\alpha_{23}\alpha_{31} -$$

$$-\alpha_{13}\alpha_{22}\alpha_{31} - \alpha_{11} \propto_{23} \alpha_{32} - \alpha_{12}\alpha_{21}\alpha_{33}.$$

PROPOSICIÓN 4.1. *El determinante de una matriz con fila (columna) a elementos nulos es nulo.*

Una matriz cuadrada se llama diagonal si son nulos todos sus elementos que no se encuentren en la diagonal principal.

PROPOSICION 4.2. *El determinante de una matriz diagonal es igual al producto de elementos de su diagonal principal*.

Una matriz cuadrada se llama *triangular* si son nulos todos sus elementos que se disponen por encima (por debajo) de su diagonal principal.

PROPOSICIÓN 4.3. *El determinante de una matriz triangular es igual al producto de los elementos de su diagonal principal*.

La demostración de las proposiciones 4.1-4.3 se deja a opción del lector.

Propiedades fundamentales de determinantes. Formúlese y demuéstrese las propiedades encontradas más a menudo.

PROPIEDAD 4.1*. Los determinantes de una matriz cuadrada A y de una matriz transpuesta ${}^{t}A$ son iguales.*

Demostración. Sea $A = \|\alpha_i\|$una matriz cuadrada de orden n y ${}^{t}A = \|\beta_{ik}\|$, donde $\beta_{ik} = \alpha_{ki}$. Entonces se tiene

$$\|A\| = \sum_{\tau\in Sn} (sgn\tau)\,\beta_{1\tau(1)} \cdots \beta_{n\tau(n)};$$

$$(1) \qquad |A| = \sum_{\tau\epsilon Sn} (sgn\tau)\alpha_{\tau(1)1} \cdots \alpha_{\tau(n)n.}$$

Dado que $\tau = \begin{pmatrix}1 & \cdots & n\\ \tau(1) & \cdots & \tau(n)\end{pmatrix}$, entonces $\tau^{-1} = \begin{pmatrix}\tau(1) & \cdots & \tau(n)\\ 1 & \cdots & n\end{pmatrix}$,

o, si se dispone en la fila superior los números en orden creciente, $\tau^{-1} = \begin{pmatrix}1 & \cdots & n\\ \tau^{-1}(1) & \cdots & \tau^{-1}(n)\end{pmatrix}\cdot$ En el producto $\alpha_{t(1)1} \cdots \alpha_{\tau(n)n}$ dispóngase los factores de manera que los primeros índices sigan un orden creciente; se obtiene entonces

$$\alpha_{\tau(1)1} \cdots \alpha_{\tau(n)n=}\alpha_{1\tau-1(1)} \cdots \alpha_{n\tau-1(n)}$$

Y la igualdad (1)se puede escribir bajo la forma

$$(2) \qquad {}^{t}A \sum_{\tau-1\in Sn}\left(sgn\tau^{-1}\right) \alpha_{1\tau-1(1)} \cdots \alpha_{n\tau-1(n)}.$$

Dado que , la permutación τ^{-1} recorre una vez todos los elementos del conjunto s_n cuando τ recorre todo los elementos de este conjunto una vez, la suma en la igualdad (2) es igual al determinante de la matriz$A$. Entonces,$|A| = |A|$. □

PROPIEDAD 4.2. *Con una permutación de dos columnas (filas) de una matriz su determinante cambia de signo*.

Demostración. Sea $A = \|\alpha_{ik}\|$ la matriz$n$ x ny $B = \|\beta_{ik}\|$ la matriz obtenida a partir de la matriz$A$ por permutación de dos columnas con índices s y t. Sea σ una transposición de S_n que convierte s en t, $\sigma = (st)$, se obtiene entonces

$\beta_{ik} = \alpha_{i\sigma(k)}$ Para $i, k \in \{1, \cdots, n\}$,

como resultado,

$$|B| = \sum_{\tau \in Sn} (sgn\tau)\beta_{1\tau(1)} \cdots \beta_{n\tau(n)} =$$

$$= \sum_{\tau \in Sn} (sgn\tau)\, \alpha_{1\sigma\tau(1)} \cdots \alpha_{n\sigma\tau(n)} \cdot$$

Según el TEOREMA 3.4, sgn $(\sigma\tau) = -$ sgn τ. Además, cuando la permutación τ recorre todos los elementos del conjunto S_n una vez, la permutación $\tau' = \sigma\tau$ recorre igualmente todos los elementos de este conjunto una vez. Se obtiene, como resultado,

$$|B| = -\sum_{\tau' \in Sn} (sgn\tau')\alpha_{1\tau'(1)} \cdots \alpha_{n\tau'(n)} = -|A|,$$

es decir $|B| = -|A|$.

PROPIEDAD 4.3 *El determinante de una matriz que posea dos columna (filas) idénticas es nulo.*

Demostración. Plantéese que la matriz$A = \|\alpha_{ik}\|$ posee dos columnas idénticas, por ejemplo, A^s=A^t. Nótese σ la transposición (st). En ese caso la igualdad $A^s = A^t$ conllevala igualdad

$$\alpha_{\tau(1)} \cdots \alpha_{n\tau(n)} = \alpha_{1\sigma\tau(1)}\alpha_{n\sigma\tau(n)}.$$

Correspóndase a cada permutación τ de S_n la permutación $\sigma\tau$. Entonces , a la permutación $\sigma\tau$ corresponde la permutación τ, ya que$\sigma(\sigma\tau) = \tau$. Llámese el conjunto $\{\tau, \sigma\tau\}$ $par\ de\ permutuacion\ correspondiente\ entre\ ellas$.El conjunto S_n se divide en pares similares permutaciones separadas de dos en dos. Estamos en presencia de una división del conjunto S_n:

$$S_{n=} \bigcup_{\tau \in An} \{\tau, \sigma\tau\},$$

Donde A_n es el conjunto de todas las permutaciones pares de grado n.

Entonces la igualdad

$|A| = \sum_{\tau \in Sn}(sgn\tau)\, \alpha_{1\tau(1)} \cdots \alpha_{n\tau(n)}$

Se puede escribir de la manera

$$|A| = \sum_{\tau \in An} [\ddot{}(sgn\tau)\, \alpha_{1\tau(1)} \cdots \alpha_{n\tau(n)} +$$

$$+(sgn\sigma\tau)\alpha_{1\sigma\tau(1)} \cdots \alpha_{n\sigma\tau(n)}].$$

A demás, según el TEOREMA 3.4,

(3) Sgn $(\sigma\tau) = -$sgn τ ·

En la base de (1) y (3) concluye que

(Sgnτ) $\alpha_{n\tau(n)} + (sgn\sigma\tau)\alpha_{\sigma\tau(1)} \cdots \alpha_{n\sigma\tau(n)} = 0.$

Así mismo, cada término de la suma (2) es nula; como resultado, $|A| == 0$.□

PROPIEDAD 4.4. *Si todos los elementos de una línea (columna) cualquiera de la matriz$A$ se multiplican por el escalar λ, el determinante de la matriz A entonces también se multiplica por el escalar λ*:

Demostración. Sean $A = \|\propto_{ik}\|$ una matriz cuadrada de orden n y B una matriz obtenida apartir de la matriz A después de la multiplicación de la i-ésima línea por el escalar λ:

$$B = \begin{bmatrix} \propto_{11} \cdots \alpha_{1n} \\ \cdots \quad \cdots \quad \cdots \\ \lambda \propto_{i1} \cdots \lambda \propto_{in} \\ \cdots \quad \cdots \quad \cdots \\ \alpha_{n1} \cdots \propto_{nn} \end{bmatrix}$$

Entonces se tiene por definición del determinante

$$|B| = \sum_{\tau \in Sn} (sgn\tau) \propto_{1\tau(1)} \cdots \left(\lambda \propto_{i\tau(i)}\right) \cdots \propto_{n\tau(n)} =$$

$$= \lambda \sum_{\tau \in Sn} (sgn\tau) \propto_{i\tau(1)} \cdots \propto_{i\tau(i)} \cdots \propto_{n\tau(n),} es\ decir\ |B| = \lambda|A|.$$

COROLARIO 4.4*. El determinante de una matriz cuya dos líneas (columnas) cualquiera son proporcionales, es nula.*

PROPIEDAD 4.5. *Si cada elemento de la i-ésima línea (columna) de una matriz cuadrada A es una suma de m términos, el determinante de la matriz$A$ entonces es igual a la suma de m determinantes, además, en la matriz del primer determinante en la i-ésima línea (i-ésima columna) se encuentran los primeros términos de la suma, en la matriz de la segunda, los segundos términos, etc., mientras que las líneas siguientes son idénticas a estas de la matriz A.*

Demostración. Supóngase que cada elemento de la i-ésima línea de la matriz A es una suma de m términos:

(1) $\propto_{ik} = \propto_{ik}^{(1)} + \cdots + \propto_{ik}^{(m)}$ $(K = 1, \cdots, m)$.

En la igualdad

$$|A| = \sum_{\tau \in Sn} [(sgn\tau) \propto_{1\tau(1)} \cdots \propto_{i\tau(i)} \cdots \propto_{n\tau(n)}$$

en cada término de la suma substituimos al factor $\propto_{i\tau(i)}$la suma de m términos según la fórmula (1) y represéntese toda la suma bajo la forma de m términos:

$$|A| = \sum_{\tau \in Sn} (sgn\tau)\alpha_{1\tau(1)} \cdots \alpha_{i\tau(i)}^{(1)} \cdots \alpha_{n\tau(n)} + \cdots$$

$$\cdots + \sum_{\tau \in Sn} (sgn\tau)\alpha_{1\tau(1)} \cdots \alpha_{i\tau(i)}^{(m)} \cdots \alpha_{n\tau(n)} .$$

Al remplazar cada una de las m sumas por el determinante se llega a la igualdad buscada

$$|A| = \begin{vmatrix} \propto_{11} \cdots \alpha_{1n} \\ \cdots \quad \cdots \\ \alpha_{i1}^{(1)} \ldots \alpha_{in}^{(1)} \\ \cdots \quad \cdots \\ \alpha_{n1} \cdots \alpha_{nn} \end{vmatrix} + \cdots + \begin{vmatrix} \propto_{11} \cdots \alpha_{1n} \\ \cdots \quad \cdots \\ \alpha_{i1}^{(m)} \ldots \alpha_{in}^{(m)} \\ \cdots \quad \cdots \\ \alpha_{n1} \cdots \alpha_{nn} \end{vmatrix} \cdot \square$$

PROPIEDAD 4.6. *Si de una columna (línea) cualquiera dela matriz del determinante ser separa otra columna (línea) de la matriz multiplicada por un escalar arbitrario, el determinante de la matriz no variará.*

Demostración. Escríbase la $n \times n$-matriz A bajo la forma

$A = (A^1, A^2, \cdots, A^n)$.

Reconózcase que la matriz B se obtiene a partir de la matriz A luego de la adjunción de la primera columna de la k-iésima columna multiplicada por el escalar λ, es decir

$B = \left(A^1 + \lambda A^k, \cdots, A^n\right)(k \neq 1)$.

Según la propiedad 4.5. El determinante de la matriz B se puede representar bajo la forma de la suma de dos términos:

$|B| = |(A^1, A^2, \cdots, A^n)| + \lambda\left|\left(A^k, A^2, \cdots, A^n\right)\right|$.

En esta suma el segundo determinante es nulo el cual posee dos columnas idénticas; por lo tanto, $|B| = |A|$. □

COROLARIO 4.5. *Si una columna (línea) cualquiera de la matriz de un determinante se añade una combinación lineal de otras columnas (líneas) de la matriz, el determinante de la matriz entonces no variara.*

PROPIEDAD 4.7. *Si una columna (línea) cualquiera de la matriz cuadrada es una combinación lineal de otras columnas (líneas) de la matriz, entonces el determinante de la matriz es nulo.*

Esta propiedad resulta fácilmente del corolario 4.5.

Ejercicios

1. ¿Cómo variara el determinante de una matriz cuadrada de orden n si cada elemento de la matriz se remplaza por su opuesto?
2. ¿Sea A un matriz cuadrada de orden $n$sobre el cuerpo F y λ un elemento de este cuerpo. Demostrar que $|\lambda A| = \lambda^n |A|$.
3. ¿Cómo variara el determinante de una matriz cuadrada de orden n un elemento complejo si cada elemento de la matriz se remplaza por su combinado?
4. ¿Los elementos de una matriz cuadrada de orden n cumplan a la condición $\propto_{ik} = \propto_{ki}$, donde $\propto_{ki}$ es un número complejo combinado de $\propto_{ik}$. Demostrar que $|A|$es un número real.
5. ¿Demostrar que el determinante de una matriz triangular es igual al producto de los elementos de la diagonal principal de la matriz.
6. ¿Cómo variara el determinante de una matriz cuadrada de orden n si cambiamos de lugar la primera y la última columna las otras columnas se desplacen hacia la izquierda conservando su disposición?
7. ¿Cómo variara el determinante de una matriz cuadrada de orden n si las columnas de la matriz se escriben en el orden inverso?
8. ¿Supónganse que el cuerpo F se cumple la desigualdad $1 + 1 \neq 0$ demostrar que el determinante de toda matriz simétrica izquierda en f de orden impar es nulo.
9. ¿Demostrar que

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_2)(x_3 - x_2).$$

10. Demostrar que tenemos el desarrollo siguiente en factores lineales del determinante de Vandermonde de orden n:

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & \cdots & \cdots & \cdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{n \geq i > k \geq 1} (x_1 - x_k).$$

11. Mostrar que si la matriz cuadrada A es inversa, tenemos

$|A^{-1}| = |A|^{-1}$.

12. Sea A una matriz cuadrada. Demostrar que $|A^k| = |A|^k$ para cada entero positivo k. Mostrar que si la matriz A es regular, tenemos $|A^k| = |A|^k$ para todo entero k

§5. Menores y complementos algebraicos.
TEOREMAs de determinantes

Menores y complementos algebraicos. Sean F un cuerpo de escalares y $A = \|\propto_{ik}\| \in F^{m\times n}$;

$$A = \begin{bmatrix} \propto_{11} \cdots \alpha_{1n} \\ \cdots\cdots\cdots \\ \alpha_{m1} \cdots \alpha_{mn} \end{bmatrix}.$$

DEFINICIÓN. *Se denomina submatriz de la matriz*A la matriz obtenida a partir de A por supresión de una colección cualquiera de sus líneas y columnas. La submatriz compuesta de k líneas k columnas se llama submatriz de orden k.

DEFINICIÓN. *El determinante de una submatriz de orden k de la matriz A es llamada menor de orden k de la matriz A*.

Los menores de orden 1 de la matriz A son sus elementos.

DEFINICIÓN. El determinante de una matriz obtenida a partir de una matriz cuadrada A eliminando la i-ésima línea y la k-e´sima columna se llama *menor del elemento* $\propto_{ik}$ *y se denota* M_{ik}. El producto$(-1)^{i+k}M_{ik}$se llama complemento álgebraico del elemento $\propto_{ik}$ y se denota A_{ik}.

Obsérvese que M_{ik} y $A_{ik} = (-1)^{i+k}M_{ik}$ son independientes de elemento $\propto_{ik}$, sin embargo, A_{ik}depende de la igualdad de la suma $i + k$.

LEMA 5.1. Sea $A \in F^{n\times n}$. Si todos los elementos de la última línea (columna) de la matriz A son nulos, excepto, probablemente, el elemento $\propto_{nn}$*, entonces se obtiente*$|A| = \propto_{nn} M_{nn}$.

Demostración. Supóngase que

(1) $\propto_{nk}$=0 para $k \in \{1, \cdots, n-1\}$.

Por definición del determinante,

$$(2)|A| = \sum_{\tau\in Sn} (sgn\tau)\alpha_{1\tau(1)} \cdots \alpha_{n-1\tau(n-1)}.\alpha_{n\tau(n).}$$

Defínase que el conjunto S'_npor igualdad

$$(3)S'_n = \{\tau \in S_n | \tau(n) = n\}.$$

Si $\tau \in S_n \setminus S'_n$ entonces en virtud de $(1) \propto_{n\tau(n)} = 0$. Por tanto en la suma (2) todos los términos que corresponde a las permutaciones τ de $S_n \setminus S'_n$ son nulos. Al eliminar en la suma (2) estos términos, se obtiene

$$(4)|A| = \alpha_{nn} \sum_{\tau\in S'_n} (sgn\tau) \propto_{1\tau(1)} \cdots \alpha_{(n-1)\tau(n-1)}.$$

Considérese la función φde un conjunto S'_n en S_{n-1}:

$$\tau = \begin{pmatrix} 1 \cdots (n-1)\, n \\ \tau(1) \cdots \tau(n-1-)n \end{pmatrix} \underset{\varphi}{\rightarrow} \begin{pmatrix} 1 \cdots (n-1) \\ \tau(1) \cdots \tau(n-1) \end{pmatrix} \tau'.$$

Así τ' es la restricción de τ enun conjunto $\{1,\cdots,n-1\}$:

(1) $\tau'(i)=\tau(i)$ para $i\in\{1,\cdots,n-1\}$,

$$\tau'=\begin{pmatrix}1\ \cdots n-1\\ \tau'(1)\ \cdots\ \tau'(n-1)\end{pmatrix}.$$

La función φ es una permutación inyectiva de un conjunto S'_n sur S_{n-1}. Como $\tau(n)=n$ para $\tau\in S'_n$, el número de inversiones en la permutación τ vale el numero de inversiones en la permutación τ'; como resultado,

(2) Sgnτ' =sgn$\tau(\tau'\in S_{n-1})$.

Sobre la base de (5) y (6) se esta en condiciones de escribir la igualdad (4) bajo la forma

$$|A|=\propto_{nn}\sum_{\tau'\in S_{n-1}}(sgn\,\tau')\propto_{1\tau'(1)}\cdots\alpha_{n-1\tau'(n-1).}$$

En esta última igualdad la suma es la menorM_{nn} que corresponde al elemento $\propto_{nn}$, es decir $|A|=\propto_{nn}.M_{nn}.\square$

LEMA 5.2. *Si todos los elementos de una línea (columna) de la matriz cuadrada A son nulos, aparte, probablemente, un elemento, $|A|$entonces es igual al producto de este elemento por su complemento álgebraico*.

Demostración. Sea $A=\|\propto_{ij}\|\in F^{n\times n}$. Supóngase que todos los elementos de la i-ésima línea de la matriz A son nulos excepto, posiblemente, el elemento $\propto_{ik}$:

(1) $\propto_{ij}=0, j\in\{1,\cdots,n\}\setminus\{k\}$.

En la matriz$A$ se desplazara la i-ésima línea hacia más adelante hasta que esta no se convierta la última cambiando sucesivamente con la línea vecina de arriba. Luego, k-ésima columna de la matriz obtenida se desplazara hacia la derecha por permutación con su vecina a la izquierda hasta que esta ocupe el último lugar. Finalmente la matriz$A$ se transforme en la matriz

$$B=\begin{bmatrix}\propto_{11}\ \ldots..\alpha_{1n}\alpha_{1k}\\ \cdots\\ \alpha_{i-1,1}\ldots\ldots\ldots..\alpha_{i-1.k}\\ \alpha_{i+1,1}\ldots\ldots\ldots\alpha_{i+1,k}\\ \ldots\ \ldots..\ldots..\\ \alpha_{n1}\ldots\ldots\alpha_{nk}\\ \alpha_{i1}\cdots\alpha_{i,k-1}\alpha_{i,k+1}\cdots\alpha_{in}\alpha_{ik}\end{bmatrix}$$

Según la condición (1), todos los elementos de la última línea de la matriz$B$ son nulos aparte, puede ser, el elemento $\propto_{ik}$.Pues, según el lema 5.1, tenemos

(2) $|B|=\propto_{ik}.M_{ik}$,

donde M_{ik} es el menor de la matriz$A$ que corresponde al elemento $\alpha_{ik.}$ La matriz Bse obtuvo a partir de la matriz$A$ por $n-i$ permutaciones de líneas y $n-k$permutaciones de columnas; así pues, según la propiedad 4.3 de los determinantes,

$|B|=(-1)^{n-i+n-k}|A|$

Y

(3) $|A|=(-1)^{i+k}|B|$.

De (2) y (3), se obtiene $|A|=(-1)^{i+k}.\alpha_{ik}.M_{ik}=\propto_{ik}A_{ik}$, es decir $|A|=\propto_{ik}A_{ik}.\square$

Desarrollo del determinante que sigue los elementos de una línea o de una columna. Al momento del cálculo de los determinantes se utiliza a menudo del TEOREMA siguiente.

TEOREMA5.3 sea $A \in F^{n\times n}$. El determinante de la matriz$A$ es igual a la suma de los productos delos elementos una columna (línea) cualquiera por sus complementos álgebraicos, es decir

(1) $|A| = \propto_{ik} A_{1k} + \cdots + \propto_{nk} A_{nk}$

$(i, k \in \{1, \cdots, n\})$.

(2) $|A| = \propto_{i1} A_{i1} + \cdots + \alpha_{in} A_{in}$

Demostración. Represéntese bajo la forma de una suma de n columnas la k-ésima columna A^kde la matriz$A$:

$$A^k = \begin{bmatrix} \propto_{ik} \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \alpha_{2k} \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \alpha_{nk} \end{bmatrix}.$$

Según la propiedad 4.5 de los determinantes, a esta representación corresponde la representación de $|A|$ bajo la forma de una suma de n determinantantes

$$|A| = \begin{bmatrix} \propto_{11} \cdots \propto_{1k} \cdots \alpha_{1n} \\ \propto_{21} \cdots 0 \cdots \alpha_{2n} \\ \cdots \quad \cdots \quad \cdots \quad \cdots \\ \alpha_{n1} \cdots 0 \cdots \alpha_{nn} \end{bmatrix} + \cdots + \begin{bmatrix} \propto_{11} \cdots \propto_{1k} \cdots \alpha_{1n} \\ \propto_{21} \cdots 0 \cdots \alpha_{2n} \\ \cdots \quad \cdots \quad \cdots \quad \cdots \\ \alpha_{n1} \cdots \alpha_{nk} \cdots \alpha_{nn} \end{bmatrix}.$$

Según el lema 5.2. El primer término de esta suma vale $\propto_{1k} A_{1k}$, el segundo, $\propto_{2k} A_{2k}$, etc. Como resultado, $|A| = \propto_{2k} A_{1k} + \propto_{2k} A_{2k} + \cdots + \propto_{nk} A_{nk}$.

De manera análoga, se demuestra la fórmula (2).□

La fórmula (1) lleva el nombre de desarrollo del determinante siguiendo los elementos de la k-ésima columna. La fórmula (2) es el desarrollo del determinante siguiendo los elementos de la, i-ésima línea.

TEOREMA5.4. Sea $|A| = \|\propto_{ij}\| \in F^{n\times n}$. La suma de los productos de los elementos de una columna (línea) cualquiera de la matriz$A$ para los complementos álgebraicos de elementos correspondiente de otra columna (línea) es nula, es decir

(3) $\propto_{1k} A_{1S} + \cdots + \alpha_{nk} A_{ns} = 0$ $(k \neq s)$,

(4) $\propto_{i1} A_{m1} + \cdots + \alpha_{in} A_{mn} = 0 (m \neq i)$,

Demostración. Demuéstrese la fórmula (3). Escríbase$A$ bajo la forma

$A = \left(A^1, \cdots, A^k, \cdots A^s, \cdots, A^n\right)$.

Al sustituir en la matriz$A$ en la s-ésima columna A^s un vector

arbitrario$b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$, resulta la matriz

$B = \left(A^1, \cdots, A^k, \cdots, b, \cdots, A^n\right)$.

Desarróllese$|B|$ siguiendo los elementos de la s-ésima columna:

$[B] = \beta_1 A_{1s} + \cdots + \beta_n A_{ns}$.

Nótese que esta igualdad se verifica para todo juego de escalares $\beta_1, \cdots \cdots, \beta_n$. en particular, que plantea $\beta_1 = \propto_{1k}, \cdots, \beta_n = \propto_{nk}$, se obtiene la igualdad

$0 = \propto_{1k} A_{1s} + \cdots + \propto_{nk} A_{ns} (k \neq s)$,

ya que la matriz$B$ tendrá dos columnas idénticas.

De manera análoga se demuestra la fórmula (4).□

Determinante de un producto de matriz. Demuéstrese en primer lugar los dos lemas.

LEMA 5.5. Si E_φ es una matriz elemental del mismo orden que una matriz cuadrada B, entonces se tiene

(1) $\left|E_\varphi B\right| = \left|E_\varphi\right||B|$y $\left|E_\varphi\right| \neq 0$.

Demostración. Cualquier matriz elemental es triangular y por tanto, su determinante es igual al producto de elementos de la diagonal principal. Por tanto, se tiene

$$(2)\left|E_\varphi\right| = \begin{cases} \lambda \; si \; E_\varphi = E_{\lambda(i)} (\lambda \neq 0), \\ 1 \; si \; E_\varphi = E_{(i)+\lambda(k);} \end{cases}$$

además,

$$(3)\; \left|E_\varphi B\right| = \begin{cases} \lambda|B| \; si \; E_\varphi = E_{\lambda(i)} \\ |B| \; si \; E_\varphi = E_{(i)+\lambda(k).} \end{cases}$$

Sobre la base de (2) y (3) se concluye que tuvo lugar (1).□

LEMA 5.6. $SiE_1, \cdots, E_s$ son de matrices elementales del mismo orden que la matriz cuadrada B, entonces se tiene

$(4)|E_1 E_2 \cdots E_s B| = |E_1||E_2| \cdots |E_s||B|$.

Demostración (conducta por recurrencia en el número s).

Según el lema 5.5, el lema 5.6 se verifica para $s = 1$. Supóngase que el lema es verdadero para $s - 1$ factores elementales y demuéstrese que se verifica también para $s$factores. Según el lema 5.5, tenemos

$|E_1(E_2 \cdots E_2 B)| = |E_1||E_2 \cdots ||E_s||B|$.

Por hipótesis de recurrencia,

$|E_2 \cdots E_s B| = |E_2||E_3| \cdots |E_s||B|$;

por tanto,

$|E_1 E_2 \cdots E_s B| = |E_1||E_2| \cdots |E_s||B|$.

La igualdad (4) es así verdadera para toda s. □

COROLARIO 5.8. $SiE_1, \cdots, E_s$son matrices elementales de un mismo orden, entonces se tiene

$|E_1 E_2 \cdots E_s| = |E_1||E_2| \cdots |E_S|$.

TEOREMA5.8. El determinante de un producto de dos matrices cuadradas es igual al producto de los determinantes de estas matrices, es decir

$|AB| = |A||B|$.

Demostración. Primer caso: las líneas de la matriz A son linealmente independientes. Según el TEOREMA 2.8, la matriz A se puede representar bajo la forma de un producto de matrices elementales $A = E_1, \cdots, E_s$, por tanto, $AB = E_1 \cdots E_s B$. Según el lema 5.6, se tiene

$|AB| = |E_1| \cdots |E_s||B|$.

Además, según el corolario 5.7,

$|AB| = |E_1 \cdots E_s| = |E_1||E_2| \cdots |E_s|$;

Como resultado, $|AB| = |A||B|$.

Segundo caso: las líneas de la matriz A son *linealmente dependientes*. En este caso se puede cambiar la matriz A por una serie de transformaciones elementales regulares en la forma de una matriz en escalar que se denotará C ; las líneas de la matriz que son linealmente dependientes, C contiene por consiguiente una línea de elementos para todo nulo. Si

$A \xrightarrow{\varphi 1 \cdots \varphi s} C$,

según la propiedad 2.4 de las matrices elementales,$E_{\varphi 1} \cdots E_{\varphi s} \cdot A = = C$. Multiplíquese esta igualdad de derecha por la matriz B:

$E_{\varphi 1} \cdots E_{\varphi s} AB = CB$.

Según el lema 5.6, $\left|E_{\varphi 1}\right| \cdots \left|E_{\varphi s}\right| |AB| = |CB|$. Como C y, por tanto, CB son matrices que poseen una línea de elementos todo nulo, se tiene$|CB| = 0$. Además, (según el lema 5.5), $\left|E_{\varphi 1}\right| \neq 0, \cdots, \left|E_{\varphi s}\right| \neq 0, \left|E_{\varphi 1}\right| \cdots \left|E_{\varphi s}\right| \neq 0$; como resultado, $|AB| = 0$. Como las líneas de la matriz A son linealmente dependientes, una de las líneas de la matriz A es por tanto una combinación lineal de otras líneas. Por eso, (según la propiedad 4.7 de los determinantes) se obtiene $|A| = 0$. Como resultado,$|A||B| == 0$

En resumen, $|AB| = |A||B|$. □

Condiciones necesarias y suficientes de la igualdad a cero del determinante. Como lo muestran los dos TEOREMAs siguientes, existen diversas condiciones mutuamente equivalentes de la igualdad a cero del determinante.

TEOREMA 5.9. El determinante de una matriz cuadrada es nula si y solo si las líneas (columnas) de la matriz son linealmente dependientes.

Demostración. Sea $A \in F^{n \times n}$. Demuéstrese que si las líneas de la matriz A son linealmente independientes, entonces $|A| \neq 0$.

En efecto, si las líneas de la matriz A son linealmente independientes, entonces según el TEOREMA 2.8, se puede representar bajo la forma de un producto de matrices elementales, es decir que $A = E_1 \cdots E_s$. Según corolario 5.7,$|A| = |E_1| \cdots |E_s|$. Además según el lema 5.5, el determinante de una matriz elemental cualquiera es diferente de cero. Por tanto, $|A| \neq 0$. Según la ley de contraposición, la afirmación demostrada es equivalente a la afirmación: si $|A| == 0$ las líneas de la matriz A son entonces linealmente dependientes.

Demuéstrese ahora la reciproca: si las líneas de la matriz cuadrada A son linealmente dependientes, entonces tenemos $|A| = 0$. En efecto, si la primera línea A_1de la matriz A no tiene elementos nulos, al menos una de las líneas $A_2 \cdots, A_n$ es entonces una combinación lineal de las otras líneas de la matriz. Por tanto, según la propiedad 4.7 de los determinantes, $|A| = 0$. □

TEOREMA 5.10. Para toda matriz cuadrada A las cuatros afirmaciones siguientes son equivalentes:

(a) $|\mathrm{A}| \neq 0$;
(b) Las líneas(columnas) de la matriz A son linealmente independientes;
(c) La matriz A es inversible;
(d) La matriz A puede ser figurada bajo la forma de un producto de matrices elementales.

Este TEOREMA resulta directamente de los TEOREMAs 5.9 y 2.8.

Ejercicios

1. Sean A Y C matrices cuadradas. Demostrar que
$\begin{vmatrix} A & 0 \\ B & C \end{vmatrix} = |A| \cdot |C|$.

2. Demostrar que
$$\begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix} = f(\omega_1) f(\omega_2) f(\omega_3),$$
donde$f = a + bx + cx^2$ y $\omega_1, \omega_2, \omega_3$ son las raíces cubicas distintas de la unidad.

3. Calcular el determinante

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix}.$$

4. Demostrar que

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2) \cdot$$

5. Al utilizar únicamente la definición del determinante, calcular el determinante de una matriz triangular A:

$$A = \begin{bmatrix} a_{11} & 0 & 0 \cdots 0 \\ a_{21} & a_{22} & 0 \cdots 0 \\ a_{31} & a_{32} & a_{33} \cdots 0 \\ \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} \cdots a_{nn} \end{bmatrix}.$$

6. Cuantas de submatrices cuadradas de orden k posee la matriz $m \times n$?

§6. Teoremas de las matrices.
Regla de Cramer

TEOREMA sobre el rango de la matriz. Estúdiese la unión del rango de la matriz con las órdenes de sus menores no nulos.

TEOREMA 6.1. El rango de una matriz no nula es igual al gran orden de los menores no nulos de la matriz.

Demostración. Sean A una matriz no nula y $A \in F^{m \times n}$. Su rango es entonces $r = r(A) > 0$.Demuéstrese que la matriz consta al menos un menor no nulo de orden r. Como $r = r(A) > 0$, la matriz A posee r líneas linealmente independientes. Sea B una submatriz de la matriz A compuesta de r líneas de la matriz A linealmente independientes, es decir que $B \in \in F^{r \times n}, r(B) = r$. Se deduce de la igualdad $r(B) = r$ que la matriz B posee r columnas linealmente independientes. Sea C una submatriz de la matriz B compuesta de r columnas linealmente independientes de la matriz B, entonces se tiene $C \in F^{r \times r}, r(C) = r$. Según el TEOREMA 5.10, $|C| \neq 0$, ya que las columnas de la matriz C son linealmente independientes. Por tanto, $|C|$ es un menor no nulo de orden r de la matriz A.

Se verifica sin duda que para $k > r(A)$, todo menor de orden k de la matriz A es nulo. En efecto, para $k > r(A)$ son linealmente dependientes todas k líneas de la matriz A. por tanto las líneas de una submatriz cuadrada $k \times k$ de la matriz A son linealmente dependientes. Como resultado, según el TEOREMA 5.9, todo menor de orden k de la matriz A es nulo.□

Matriz inversa. Sean $A \in F^{n \times n}$,

$$A = \begin{bmatrix} \propto_{11} \propto_{12} & \cdots \propto_{1n} \\ \propto_{21} \propto_{22} & \cdots \propto_{2n} \\ \cdots & \cdots \\ \propto_{n1} \propto_{n2} & \cdots \propto_{nn} \end{bmatrix}$$

yA_{ik} el complemento álgebraico del elemento $\propto_{ik}$.

Se llama *matriz adjunta* de A la matriz

$$A^* = \begin{bmatrix} A_{11}\, A_{21} \cdots A_{n1} \\ A_{12} A_{22} \cdots A_{n2} \\ \cdots\cdots\cdots \\ A_{1n}\, A_{2n} \cdots A_{nn} \end{bmatrix}.$$

En virtud de los TEOREMAs 5.3 y 5.4,

$$A_i(A^*)^{\mathrm{k}} = (\propto_{i1}, \cdots, \propto_{in}) \begin{bmatrix} A_{ki} \\ \vdots \\ A_{kn} \end{bmatrix} = \propto_{i1} A_{k1} + \cdots + \propto_{in} A_{kn} =$$

$$= \begin{cases} |A| si\ i = k, \\ 0\ \ si\ i \neq k, \end{cases}$$

Por tanto,

$$AA^* = \begin{vmatrix} |A| & 0 & \cdots & 0 \\ 0 & |A| & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & |A| \end{vmatrix} = |A|E (E \text{ es una matriz unidad});$$

(1) $A\left(|A|^{-1}A^*\right)A = E$,si $|A| \neq 0$.

Cálculos similares que conducen a las igualdades

$A^*A = |A|E$,

(2) $(|A|^{-1}A^*)A = E$, si $|A| \neq 0$.

Las igualdades (1) y (2) muestran que las matrices A y $|A|^{-1}A^*$ son mutualmente invertidas. Se demostró el TEOREMA siguiente.

TEOREMA 6.2. Si el determinante de una matriz cuadrada A es diferente de cero, la matriz A entonces es inversible y $A^{-1} = |A|^{-1}A^*$.

Regla de cramer. Considérese un sistema de n ecuaciones lineales de n variables

$\propto_{11} x_1 + \cdots + \propto_{1n} x_n = \beta_1,$

. . . . . .

$\propto_{n1} \propto_1 + \cdots + \propto_{nn} \propto_n = \beta_n$

En el cuerpo F. Nótese para A la matriz fundamental de este sistema: $A = \|\propto_{ik}\|$.

TEOREMA 6.3. Si $|A| \neq 0$ el sistema de ecuaciones lineales (1) posee una solución única que expresa las fórmulas

(2) $\propto_1 = |A|^{-1}(\beta_1 A_{11} + \cdots + \beta_n A_{n1}), \cdots$

$$\cdots, x_n = |A|^{-1}(\beta_1 A_{1n} + \cdots + \beta_n A_{nn}).$$

Demostración. Al plantear $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$.

Escríbase el sistema (1) bajo la forma de una ecuación matricial.

(3) $A\mathrm{X} = b$,

equivalentes al sistema (1). Según el TEOREMA 5.9, se deduce de la condición $|A| \neq 0$ que las líneas de la matriz A son linealmente independientes y que los sistemas (3) y (1) admiten una solución única $x = A^{-1}b$.

De ahí, puesto que (según el TEOREMA 6.2) $A^{-1} = |A|^{-1}A^*$, se obtiene

$$A^{-1}b = |A|^{-1}\begin{bmatrix} A_{11} \cdots A_{n1} \\ \cdots\cdots\cdots \\ A_{1n} \cdots A_{nn} \end{bmatrix}\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} =$$

$$= |A|^{-1}\begin{bmatrix} \beta_1 A_{11} + \cdots + \beta_n A_{n1} \\ \cdots\cdots\cdots\cdots \\ \beta_1 A_{1n} + \cdots + \beta_n A_{nn} \end{bmatrix}$$

Y

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} |A|^{-1}(\beta_1 A_{11} + \cdots + \beta_n A_{n1}) \\ \cdots\cdots\cdots\cdots \\ |A|^{-1}(\beta_1 A_{1n} + \cdots + \beta_n A_{nn}) \end{bmatrix}.$$

De esta última igualdad resultan las fórmulas (2).□

Las fórmulas (2) habitualmente se denominan *fórmulas de Cramer*, mientras que el TEOREMA 6.3 se llama *regla de Cramer*.

Nótese $A(k)$la matriz obtenida a partir de la matriz A sustituyendo a la k-ésima columna de los términos libres del sistema (1)

$$A(1)= \begin{bmatrix} \beta_1 \propto_{12} \cdots \propto_{1n} \\ \cdots\cdots\cdots \\ \beta_n \propto_{n2} \cdots \propto_{nn} \end{bmatrix}, \cdots, A(n) = \begin{bmatrix} \propto_{11} \cdots \propto_{1n-1} \beta_1 \\ \cdots\cdots\cdots\cdots \\ \propto_{n1} \cdots \propto_{nn-1} \beta_n \end{bmatrix}.$$

Al desarrollar el determinante de la matriz $A(k)$que sigue los elementos de la k-ésima columna, se obtiene
$|A(k)| = \beta_1 A_{1k} + \cdots + \beta_n A_{nk} (k = 1, \cdots, n)$.
Estas igualdades permiten reformular el TEOREMA 6.3 de la manera siguiente.

TEOREMA 6.4. Si $|A| \neq 0$ *el sistema de ecuaciones lineales (1) admite una solución única explicitadas para las fórmulas*

(2)$x_1 = \frac{|A(1)|}{|A|}, \cdots, x_n = \frac{|A(n)|}{|A|}$.

Condiciones para las cuales un sistema de n ecuaciones lineales homogéneas de n variables admite soluciones no nulas.

TEOREMA 6.5. Un sistema de n ecuaciones lineales homogéneas de n variables tiene soluciones no nulas si y solo si el determinante de la matriz del sistema es nulo.

Demostración. Sea dada un sistema de ecuaciones lineales homogéneas

$\propto_{11} x_1 + \cdots + \propto_{1n} x_n = 0,$
(1). . . . . .
$\propto_{n1} x_1 + \cdots + x_{nn} x_n = 0,$
$A = \| \propto_{ik} \|$ Siendo la matriz de este sistema. El sistema (1) tiene soluciones no nulas si y solo si las columnas de la matriz A son linealmente dependientes. Las columnas de la matriz A son linealmente dependientes si y solo si $|A| = 0$. como resultado, el sistema (1) admite soluciones no nulas si y solo si $|A| = 0$.□

COROLARIO 6.6. La ecuación matricial$AX = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, donde

$A \in F^{n \times n}, x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ *tiene soluciones no nulas si y solo si* $[A] = 0$.

Ejercicios

1. Mostrar que el rango de un producto de la matriz no sobrepase el de cada uno de los factores.
2. Sean Ay B matrices cuadradas de orden n. Mostrar que las ecuaciones AX$= B$y X$A = B$,donde X es una matriz buscada, son insuperables cuando el rango de la matriz B sobrepase la de A.
3. Sean A y B de las matrices rectangulares que posee el mismo número de líneas y C la matriz obtenida de la matriz A por adjunción de derecha de la matriz B. Demostrar que la ecuación de las matriciales$A$X$= B$,donde X es la matriz buscada, tiene una solución si y sólo si el rango de la matriz A es igual a la de la matriz C.
4. Sea AX$= B$una ecuación matricial, donde X es la matriz buscada, y X su solución cualquiera. Demostrar que cada solución de la ecuación matricial se puede escribir bajo la forma X_0+Y, donde Y es la solución de la ecuación homogénea A Y$= 0$,y recíprocamente.
5. Buscar todas las matrices complejas en las que las cuadradas son iguales a una matriz nula.
6. Estudiar la ecuación X$A = 0$,donde A es la matriz dada y X la matriz buscada de segundo orden.
7. Buscar todas las matrices complejas del segundo orden en las que las cuadradas son iguales a una matriz unidad.
8. Sean A y Bmatrices $m \times n$. Demostrar que $r(A + B) \leq r(A) + +r(B)$*).
9. Sean A y B matrices que posee un mismo número de líneas y C una matriz obtenida al adjuntar a A todas las columnas de la matriz B.
   Demostrar que $r(C) \leq r(A) + r(B)$.
10. Mostrar que si el producto AB es una matriz regular, entonces las matrices A y B son igualmente regulares.
11. Sea A una matriz cuadrada regular de orden n. Mostrar que para toda, matriz cuadrada B de orden n, las matrices AB, By BA tienen el mismo rango.
12. Sean A, B de las matrices $n \times n$ de rango r y s respectivamente. Demostrar que $r(AB) \geq r + s - n$.
13. Demostrar que la matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$es inversible si y solo si $ad - bc \neq 0$.
14. Demostrar que si la matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$es inversible, entonces $A^{-1} = = (ad - bc)^{-1}.\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

15. Demostrar que cada matriz triangular A (en el cuerpo F) a los elementos no nulos en la diagonal principal es inversibley la matriz A^{-1} es una matriz triangular.

16. Sean A, B de las matrices $n \times n$ regulares en el cuerpo F. Mostrar que las igualdades $AB = BA, AB^{-1} = B^{-1}A, A^{-1}B = BA^{-1}, A^{-1}B^{-1} = B^{-1}A^{-1}$ son equivalentes entre estas.

17. Sea A una matriz $m \times n$ en el cuerpo F. Demostrar que:

(a) Existe una matriz $n \times m$ tal queX$A = E$,donde E es una matriz $m \times m$ unidad si y solo si el rango de A vale n;

(b) Existe una matriz $n \times m$ tal que AY$= E$,donde E es una matriz $m \times m$ unidad si y solo si el rango de A vale m.

18. Sea Auna matriz triangular $n \times n$ (en el cuerpo F) cuyos elementos de la diagonal principal valen 1. Supóngase que $B = A - E$, donde Ees una matriz de unidad $n \times n$. Demostrar que:

(a) $B^{n+1} = 0$;

(b) La matriz A es inversibley $A^{-1} = (E + B)^{-1} = E - B + B^2 - \cdots\cdots + (-1)^{nBn}$;

(c) $(E - B)^{-1} = E + B + B^2 + \cdots + B^n$.

19. Sea A una matriz triangular (en el cuerpo) de elementos no nulos en la diagonal principal. Demostrar que la matriz Aes inversible.

20. Buscar las condiciones que debe cumplir una matriz cuadrada de elementos enteros para que todos los elementos de la matriz invertida sean enteros.

21. Sean A una matriz $n \times n$ cuadrada y A^* la matriz adjunta de A.

Demostrar que:

(a) Si Aes una matriz singular, entonces la matriz AA^* es nula;
*) $r(A)$es aquí el rango de la matriz A.
(b) $A^* = |A|A^{-1}$ si A es una matriz inversible;
(c) A^* es una matriz singular si y solo si la matriz A es singular;
(d) $|A^*| = |A|^{n-1}$;
(e) si la matriz A es simétrica o simétrica izquierda, entonces A^* es también simétrica o simétrica izquierda;
(f) si A es una matriz triangular, entonces A^* es también triangular.
22. sea A^* una matriz triangular adjunta de la matriz $n \times n$ A. Demostrar que:
(a) si el rango $A < n - 1$, entonces A^* es una matriz nula;
(b) si A es el rango $n - 1$, entonces el rango de A^* es 1;
(c) si A tiene el rango n, el rango de A^* entonces es también n.
23. sea A una matriz triangular $n \times n$ en el cuerpo F. demostrar que la matriz A
es inversible si y solo si todos los elementos de la matriz A al colocarse en la diagonal principal son diferentes de cero.

CAPITULO VII
ESPACIOS VECTORIALES

§ 1. Espacios vectoriales

Noción del espacio vectorial. Sean$\mathcal{F}$ un cuerpo y F su conjunto de base. Los elementos del conjunto F serán denominados *escalares*, mientras que$\mathcal{F}$ será nombrado *cuerpo de escalares*.

Sean V un conjunto no vacío y $F \times V$ el producto directo de los conjuntos F y V. Sea dada la función

$\omega: F \times V \to V$

asociando a cada pareja$\langle \lambda, a \rangle$de $F \times V$ un elemento único del conjunto$V$se denota λa y llamada *producto del escalar* λ *y del elemento* a. Si el escalar λ es fijo, la funciónω induce la función

$\omega_\lambda: \{\lambda\} \times V \to V$

que es la restricción ωen el conjunto$\{\lambda\} \times V$.La función ω_λ con λ fija también se puede asimilar a una operación en un lugar (simple) $V \to V$ que asocia a cada elemento $\mathbb{a}$ de$V$ un elementoλade$V$.Así, $\omega_\lambda a = \lambda a$para toda a de V.

Ejemplo. Sean$\mathcal{F}$ un cuerpo, $V = F^n$y λ un elemento fijo de F. Nótese $\omega_\lambda$la aplicación V en V que asocia a cada vector $(\alpha_1, \dots \alpha_n)$de F^nel vector$(\lambda\alpha_1, \dots \lambda\alpha_n)$de F^n *llamado producto del escalar y del vector aritmético*$(\alpha_1, \dots \alpha_n)$.

Definición. El conjunto Vcon la operación binaria dada sobre $+$ (llamada suma) y la operación de multiplicación de los elementos del cuerpo de los escalares $\mathcal{F}$ por los elementos del conjunto V se llama *espacio vectorial sobre los cuerpos* F si para todos a, b de Vy α, βde F satisfacen las condiciones (axiomas) siguientes:

(1). El álgebra$\langle V, +, - \rangle$, donde $-$ es la operación de multiplicación por el escalar(-1) de los elementos de V, es un grupo abeliano;

(2). $(\alpha\beta)\,\mathrm{a} = \alpha\,(\beta\mathrm{a})$;

(3). $\alpha(\mathrm{a} + \mathrm{b}) = \alpha\mathrm{a} + \alpha\mathrm{b}$;

(4). $(\alpha + \beta)\mathrm{a} = \alpha\mathrm{a} + \beta\mathrm{a}$;

(5). $1 \cdot \mathrm{a} = \mathrm{a}$.

El espacio vectorial con el conjunto de base V se denota$\mathcal{V}$. Así, el espacio vectorial$\mathcal{V}$ es un álgebra con el conjunto de base V, en el cual la operación binaria $+$ y las operaciones simplesω_λ(multiplicación por el escalar λ de F) son operaciones principales, es decir que cualesquiera que sean

$\mathcal{V} = \langle V, +, \{\omega_\lambda \mid \lambda \in F\} \rangle$,

Las operaciones principales satisfacen a las condiciones$(1) - (5)$llamadas *axiomas* del *espacio vectorial.*

El grupo$\langle V, +, - \rangle$se denomina *grupo aditivo del espacio vectorial*$\mathcal{V}$.

El cero de este grupo se llama *vector nulo del espacio vectorial*$\mathcal{V}$.

Los elementos del conjunto V se llaman *vectores del espacio vectorial* $\mathcal{V}$. Los vectoresay(-1)ase denomina n*o puestos el uno con el otro*.

Ejemplos de espacios vectoriales. 1. Sea $\mathcal{F}^n$un espacio aritmético en n dimensiones sobre el cuerpo$\mathcal{F}$; $\mathcal{F}^n$es un espacio vectorial sobre el cuerpo$\mathcal{F}$. Casos particularmente importantes: $\mathcal{Q}^m, \mathcal{R}^n, \mathcal{C}^n$.

2. El conjunto de todos los vectores del plano es un espacio vectorial sobre el cuerpo $\mathcal{R}$ de los números reales respecto a las operaciones de suma y multiplicación por números reales.

3. Sea $F^{m \times n}$un conjunto de todas las matrices$m \times n$ sobre el cuerpo$\mathcal{F}$. El álgebra$\langle F^{m \times n}, +, \{\omega_\lambda \mid \lambda \in F\} \rangle$, donde $+$es la operación de suma de las matrices y $\omega_\lambda$la operación de multiplicación de las matrices por el escalar λ, es un espacio vectorial sobre el cuerpo$\mathcal{F}$. Se le llama *espacio vectorial de matrices*$m \times n$ sobre el cuerpo $\mathcal{F}$.

4. El conjunto de todas las aplicaciones del conjunto $\mathbb{R}$en$\mathbb{R}$ es un espacio vectorial sobre el cuerpo$\mathcal{R}$ respecto a las operaciones de suma de las funciones y multiplicación de las funciones por números reales.

5. El conjunto $\mathbb{C}$ de todos los números complejos es un espacio vectorial sobre el cuerpo$\mathcal{R}$respecto a las operaciones de suma de los números complejos y de multiplicación por los números reales.

Propiedades elementales de los espacios vectoriales.

*TEOREMA*7.1. *Sean*$\mathcal{V}$ *un espacio vectorial sobre el cuerpo*$\mathcal{F}$, $\mathbb{a}, \mathbb{b} \in V$y $\alpha, \beta \in F$.

Entonces,

(1). *Si*$\mathbf{a}\ \mathbf{b} = \mathbf{a}$,*entonces*$\mathbf{b} = \mathbf{0}$*;*

(2). $\mathbf{0} \cdot \mathbf{a} = \mathbf{0}$*;*

(3). $\alpha \cdot \mathbf{0} = \mathbf{0}$*;*

(4). *Si*$\mathbf{a} + \ \mathbf{b} = \mathbf{0}$*, entonces*$\mathbf{b} = (-1)\mathbf{a} = -\mathbf{a}$*;*

(5). *Si* $\alpha \cdot \ \mathbf{a} = \alpha \cdot \mathbf{b}$*y* $\alpha \neq \mathbf{0}$*, entonces* $\mathbf{a} = \mathbf{b}$*;*

(6). *Si* $\alpha \cdot \ \mathbf{a} = \mathbf{0}$*, entonces* $\alpha = \mathbf{0}$*o*$\mathbf{a} = \mathbf{0}$*;*

(7). *Si* $\alpha\ \mathbf{a} = \beta\ \mathbf{a}$*y* $\mathbf{a} \neq \mathbf{0}$*, entonces* $\alpha = \beta$.

Demostración.(1)Dado que$\mathbf{0}$ es un cero del grupo aditivo del espacio$\mathcal{V}$, entonces$\mathbf{a} + \mathbf{0} = \mathbf{a}$. También, se puede escribir la igualdad$\mathbf{a} + \mathbf{b} = \mathbf{a}$bajo forma$\mathbf{a} + \mathbf{b} = \mathbf{a} + \mathbf{0}$. Según la ley de simplificación (que concierne los grupos) quiere decir que$\mathbf{b} = \mathbf{0}$.

(2). Según el axioma (4)del espacio vectorial, se obtiene$\mathbf{0} \cdot \mathbf{a} + \mathbf{0} \cdot \mathbf{a} = (\mathbf{0} + \mathbf{0})\mathbf{a} = \mathbf{0} \cdot \mathbf{a}$, es decir$\mathbf{0} \cdot \mathbf{a} + \mathbf{0} \cdot \mathbf{a} = \mathbf{0} \cdot \mathbf{a}$. Según la propiedad$(1)$, quiere decir que $\mathbf{0} \cdot \mathbf{a} = \mathbf{0} \cdot \mathbf{a}$

(3). Según el axioma (3) del espacio vectorial, $\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \alpha\ (\mathbf{0} + \mathbf{0}) = \alpha \cdot \mathbf{0}$, es decir $\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \alpha \cdot \mathbf{0}$. De la propiedad (1), se desprende la igualdad $\alpha \cdot \mathbf{0} = \mathbf{0}$.

(4). Dado que$\mathbf{a} + (-1)\mathbf{a} = \mathbf{0}$, la igualdad $\mathbb{a} + \mathbf{b} = \mathbf{0}$ se puede escribir bajo forma $\mathbf{a} + \mathbf{b} = \mathbf{a} + (-1)\mathbf{a}$. Según la ley de simplificación (que concierne los grupos), se deduce que $\mathbf{b} = (-1) \cdot \mathbf{a}$.

(5). Para $\alpha = \mathbf{0}$ de $\alpha\mathbf{a} = \alpha\mathbf{b}$, se deduce que $\alpha^{-1}(\alpha\ \mathbf{a}) = \alpha^{-1}(\alpha\ \mathbf{b})$ y, en virtud del axioma $(2)\mathbf{a} = \mathbf{b}$.

(6). Como $\alpha\ \mathbf{0} = \mathbf{0}$, se puede escribir la igualdad $\alpha\ \mathbb{a} = \mathbf{0}$ bajo la forma $\alpha\ \mathbf{a} = \alpha \cdot \mathbf{0}$. Para $\alpha \neq \mathbf{0}$, según la propiedad (5), se obtiene que $\mathbf{a} = \mathbf{0}$.

(7). Al adjuntar $(-\beta\mathbf{a})$ a los dos miembros de igualdad $\alpha\ \mathbf{a} = \beta\mathbf{a}$, se obtienen $\alpha\ \mathbf{a} + (-\beta)\mathbf{a} = \mathbf{0}$,$(\alpha - \beta)\mathbf{a} = \mathbf{0}$.Para $\mathbf{a} \neq \mathbf{0}$, según la propiedad (6), se deduce que $\alpha - \beta = \mathbf{0}$ y $\alpha = \beta$.

Dependencia e independencia lineales de un sistema de vectores.

Sea $\mathcal{V}$ un espacio vectorial sobre los cuerpos $\mathcal{F}$. Se dice que el sistema de los vectores $\mathbf{a}_{1,} \ldots, \mathbf{a}_m$ del espacio es *linealmente dependiente* si existen los escalares $\lambda_{1,} \ldots, \lambda_m \in F$ no cualquier nulo tal como $\lambda_1\mathbf{a}_1 + \cdots + \lambda_m\mathbf{a}_m = \mathbf{0}$.

El sistema de vectores $\mathbf{a}_{1,} \ldots, \mathbf{a}_m$ del espacio $\mathcal{V}$ se denomina *linealmente independiente* si para cualquier escalar $\lambda_{1,} \ldots, \lambda_m \in F$ de la igualdad $\lambda_1\mathbf{a}_1 + \cdots + \lambda_m\mathbf{a}_m = \mathbf{0}$ resultan las igualdades $\lambda_1 = \mathbf{0}, \ldots, \lambda_m = \mathbf{0}$.

Para los espacios vectoriales arbitrarios son verdaderos: los enunciados y las Demostraciónes de las propiedades y los TEOREMAs del § 5.1 sobre la dependencia e independencia lineal de los sistemas (propiedades $5.1.1 - 5.1.5$, TEOREMAs y corolarios $5.1.2 - 5.1.5$); las DEFINICIÓNes y TEOREMAs de§ 5.1 sobre los sistemas equivalentes de vectores y sus Demostraciónes (TEOREMA $5.1.6 - 5.1.8$); los TEOREMAs y proposiciones (y sus Demostraciónes) del § 5.1 sobre la base y el rango de un sistema finito de vectores (TEOREMAs 5.1.9, TEOREMAs y proposiciones $5.1.10 - 5.1.15$).

Ejercicios

1. Sea $\mathcal{F} = z_2$ un cuerpo de clases residuales módulo 2. ¿Cuantos vectores contiene el espacio vectorial $\mathcal{V} = \mathcal{F}^n$, espacio aritmético en n dimensiones sobre el cuerpo $\mathcal{F}$?

2. Sea $\mathcal{F}$ un cuerpo de los escalares y $\mathcal{F}^{2\times2}$el conjunto de toda matriz 2×2 sobre el cuerpo $\mathcal{F}$. Demostrar que el álgebra
$\langle F^{2\times2}, +, -, \{\omega_\lambda \mid \lambda \in F\}\rangle$,
donde $+$ es la operación de adición de las matrices y ω_λ la operación de multiplicación por el escalar λ, es un espacio vectorial sobre el cuerpo $\mathcal{F}$.

3. Sea $\mathbb{C}^{\mathbb{R}}$ el conjunto de todas aplicaciones del conjunto $\mathbb{R}$ de los números reales en el conjunto de $\mathbb{C}$ de números complejos. Demostrar que el álgebra
$\langle \mathbb{C}^{\mathbb{R}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbb{C}\}\rangle$,
donde $+$ es la operación de adición de las funciones y ω_λ la operación de multiplicación por el escalar λ, $\big((\lambda \mathfrak{f})(x) = \lambda \mathfrak{f}(x), \lambda \in \mathbb{C}\big)$ y $-\mathfrak{f} = (-1) \cdot \mathfrak{f}$, es un espacio vectorial sobre el cuerpo de los números complejos.

4. Sea $\mathbb{R}^{\mathbb{C}}$ el conjunto de todas las funciones del conjunto $\mathbb{C}$ de los números complejos en el conjunto $\mathbb{R}$ de los números reales. Demostrar que el álgebra
$\langle \mathbb{R}^{\mathbb{C}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbb{R}\}\rangle$,
Donde $+$ es la operación de adición de las matrices y ω_λ la operación de multiplicación por el escalar λ, es un espacio vectorial sobre el cuerpo $\mathcal{R}$ de los números reales.

5. Sea $\mathcal{R}$ un cuerpo de números reales y Q un cuerpo de los números racionales. Demostrar que el álgebra
$\langle \mathbb{R}, +, -, \{\omega_\lambda \mid \lambda \in Q\}\rangle$
donde $+$ es una operación banal de adición de los números reales y ω_λ una operación banal de multiplicación por un número racional λ, es un espacio vectorial sobre el cuerpo Q.

6. Sean $\mathbb{C}$ el conjunto de todos los números complejos y Q el conjunto de todos los números racionales. Mostrar que el álgebra
$\langle \mathbb{C}, +, -, \{\omega_\lambda \mid \lambda \in Q\}\rangle$
donde $+$ es una adición banal de los números complejos y ω_λ una operación de multiplicación por el escalar λ (por el numero racional λ), es un espacio vectorial sobre el cuerpo Q.

7. Sea $\mathcal{V}$ el conjunto de todas las funciones reales doblemente derivables $\mathfrak{f} : \mathbb{R} \to \mathbb{R}$, que satisface a la ecuación diferencial $\mathfrak{f}^n + \mathfrak{f} = 0$. Demostrar que el álgebra
$\langle \mathcal{V}, +, -, \{\omega_\lambda \mid \lambda \in \mathbb{R}\}\rangle$,
Donde $+$ es una operación de adición y ω_λ una operación de multiplicación por un escalar (un número real), es un espacio vectorial sobre el cuerpo $\mathcal{R}$.

8. Sea$\mathcal{V}$ el conjunto de todas las funciones reales n vez derivables $\mathfrak{f} : \mathbb{R} \to \mathbb{R}$, que satisfacen a la condición (en la ecuación diferencial)
$\mathfrak{f}^{(n)} + \lambda_{n-1}\mathfrak{f}^{(n-1)} + \cdots + \lambda_1\mathfrak{f}' + \lambda_0\mathfrak{f} = 0$,
donde $\mathfrak{f}^{(\mathcal{K})}$ es la $\mathcal{K}$-esima derivada de la función $\mathfrak{f}$ y $\lambda_0, \ldots, \lambda_{n-1} \in \mathbb{R}$. Demostrar que el álgebra $\langle \mathcal{V}, +, -, \{\omega_\lambda \mid \lambda \in \mathbb{R}\}\rangle$, donde $+$ es una operación de adición de la funciones y ω_λ una operación de multiplicación por el escalar λ, es un espacio sobre el cuerpo $\mathcal{R}$.

9. Mostrar que el sistema compuesto de un solo vector es linealmente independiente si y solo si el vector no es nulo.

10. Demostrar que un sistema de dos vectores es linealmente independiente si y solo si uno de los vectores es deducido de otro por multiplicación por un escalar.

11. Mostrar que los vectores $(\alpha, \beta)(\gamma, \delta)$de un espacio vectorial aritmético en dos dimensiones son linealmente independientes si y solo si $\alpha\delta - \beta\gamma = 0$.

12. ¿En cuales condiciones deben satisfacer los escalares α, β, γ para que el sistema de los vectores$(1, \alpha, \alpha^2), (1, \beta, \beta^2), (1, \gamma, \gamma^2)$de un espacio vectorial aritmético en tres dimensiones sobre el cuerpo numérico $\mathcal{F}$ sea linealmente independiente?

13. Sea $\mathcal{V}$ un espacio vectorial sobre el cuerpo numérico $\mathcal{F}$. Mostrar que si los vectores $\mathbf{a}, \mathbf{b}, \mathbf{c}$ del espacio $\mathcal{V}$ son linealmente independientes, entonces los vectores $\mathbf{a} + \mathbf{b}, \mathbf{a} + \mathbf{a}, \mathbf{b} + \mathbf{c}$también son linealmente independientes. ¿Se cumple en caso de que el cuerpo de los escalares $\mathcal{F}$ conste de dos elementos?

14. Sea $\mathcal{V} = \mathcal{F}^n$ un espacio aritmético en n dimensiones sobre el cuerpo $\mathcal{F}$. Mostrar que el sistema de los vectores $\mathbf{a}_1, \dots, \mathbf{a}_m$ del espacio $\mathcal{V}$ es linealmente independiente si y solo si el rango de la matriz $m \times n$ en las líneas $\mathbf{a}_1, \dots, \mathbf{a}_m$ vale m.

15. Mostrar que un sistema de vectores no nulos $\mathbf{a}_1, \dots, \mathbf{a}_m$ del espacio vectorial $\mathcal{V}$ es linealmente independiente si y solo si $a_\mathcal{K} \notin L(\mathbf{a}_1, \dots, \mathbf{a}_{\mathcal{K}-1})$ para todos $\mathcal{K} = 2,3, \dots, m$.

16. Sean $\mathcal{F}$ un cuerpo finito compuesto de ρ elementos y $\mathcal{V} = \mathcal{F}^n$. ¿Cuántos sistemas distintos linealmente independientes que constan de $\mathcal{K}$ vectores $(\mathcal{K} < n)$ hay en el espacio $\mathcal{V}$?

17. Sean $\mathcal{F}$ un cuerpo y A la matriz $n \times n$ sobre $\mathcal{F}$. Demostrar que para un m suficientemente grande el sistema de las matrices $\mathrm{E}, \mathrm{A}, \mathrm{A}^2, \dots, \mathrm{A}^m$, donde E es una matriz unidad $n \times n$, es linealmente dependiente sobre el cuerpo $\mathcal{F}$.

18. Sea $\mathbf{a}_1, \dots, \mathbf{a}_m \in Q$. Demostrar que el sistema de los vectores $\mathbf{a}_1, \dots, \mathbf{a}_m$ es linealmente independiente en el espacio $\mathcal{R}^n$ si y solo si es linealmente independiente en el espacio Q^n.

19. Sea $\mathcal{F}$ un cuerpo finito compuesto de ρ elementos. ¿Cuántos sub-espacios distintos en $\mathcal{K}$ dimensiones $(\mathcal{K} < n)$ posee el espacio vectorial $\mathcal{F}^n$?

§ 2. Sub-espacios de un espacio vectorial

Sub-espacio vectorial. Sean $\mathcal{V}$ un espacio vectorial sobre el cuerpo $\mathcal{F}$ y $\mathbb{U} \subset V$. El conjunto $\mathbb{U}$ se denomina *cerrado* en $\mathcal{V}$ si es cerrado relativamente en las operaciones principales de $\mathcal{V}$, operaciones de adición y de multiplicación por un escalar, es decir que para todos $\mathbf{a}, \mathbf{b}$ de $\mathbb{U}$ y λ cualquiera de F, se tiene $\mathbf{a} + \mathbf{b} \in \mathbb{U}$ y $\lambda\mathbf{a} \in \mathbb{U}$.

DEFINICIÓN. Se llama *sub-espacio de un espacio vectorial* $\mathcal{V}$ toda sub-álgebra del espacio $\mathcal{V}$ considerado como un álgebra.

Sea $\mathcal{V} = \langle V, +, \{\omega_\lambda | \lambda \in F\}\rangle$ un espacio vectorial sobre $\mathcal{F}$. Sean $\mathcal{U}$ un sub-álgebra del espacio $\mathcal{V}$ y $\mathbb{U}$ son conjuntos de base. Entonces $\mathbb{U}$ es un sub-conjunto no vacio del conjunto V cerrado en $\mathcal{V}$. Sean $\oplus$ y ω_λ las restricciones de las operaciones principales " $+$ " y ω_λ del espacio $\mathcal{V}$ en el conjunto $\mathbb{U}$, es decir

$\mathbf{a} \oplus \mathbf{b} = \mathbf{a} + \mathbf{b}$ para todos $\mathbf{a}, \mathbf{b}$ de $\mathbb{U}$,

$\omega'_\lambda \mathbf{a} = \omega_\lambda \mathbf{a} = \lambda\mathbf{a}$ para todo $\mathbf{a}$ de $\mathbb{U}$;

Entonces,

(1). $\mathcal{U} = \langle \mathbb{U}, \oplus, \{\omega'_\lambda | \lambda \in F\}\rangle$.

No obstante, en lugar de la notación (1), se escribe

$\mathcal{U} = \langle \mathbb{U}, +, \{\omega_\lambda | \lambda \in F\}\rangle$.

Indíquese las propiedades siguientes de un sub-espacio.

PROPIEDAD 2.1. Si $\mathcal{V}$ es un espacio vectorial sobre el cuerpo $\mathcal{F}$, entonces, todo su sub-espacio constituye un espacio vectorial sobre el cuerpo $\mathcal{F}$.

PROPIEDAD 2.2. Si $\mathcal{W}$ es un sub-espacio del espacio vectorial $\mathcal{U}$ y $\mathcal{U}$ un sub-espacio del espacio vectorial $\mathcal{V}$, entonces $\mathcal{W}$ es un sub-espacio del espacio $\mathcal{V}$.

Se llama *intersección de los sub-espacios* $\mathcal{U}_1, \dots, \mathcal{U}_m$ del espacio vectorial $\mathcal{V}$ el sub-espacio $\mathcal{V}$ con el conjunto de base $\mathbb{U}_1 \cap \mathbb{U}_2 \cap, \dots, \cap \mathbb{U}_m$. Se define de manera análoga la intersección de un conjunto infinito de sub-espacios del espacio $\mathcal{V}$.

PROPIEDAD 2.3. Una intersección de todo conjunto de sub-espacios del espacio vectorial $\mathcal{V}$ es un sub-espacio del espacio $\mathcal{V}$.

Las propiedades 2.2 y 2.3 se derivan de los TEOREMAs 3.1.7 y 3.1.9 respectivamente.

Envoltura lineal de un conjunto de vectores. Sea $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ un conjunto finito de vectores del espacio vectorial $\mathcal{V}$. El vector $\lambda_1\mathbf{a}_1 + \cdots + \lambda_n\mathbf{a}_n$ se denomina *combinación lineal de los vectores* $\mathbf{a}_1, \dots, \mathbf{a}_n$ con coeficientes en $\mathcal{F}$.

DEFINICIÓN. El conjunto $\{\lambda_1\mathbf{a}_1+\cdots+\lambda_n\mathbf{a}_n|\lambda_1,\ldots,\lambda_n\in F\}$ de todas las combinaciones lineales de los vectores $\mathbf{a}_1,\ldots,\mathbf{a}_n$con coeficientes en F se denomina *envoltura lineal de los vectores* $\mathbf{a}_1,\ldots,\mathbf{a}_n$ y se denota $L(\mathbf{a}_1,\ldots,\mathbf{a}_n)$.

Se constata sin duda que la envoltura lineal de los vectores está cerrada en $\mathcal{V}$, es decir esta cerrada relativamente en todas las operaciones principales del espacio $\mathcal{V}$ (adición y multiplicación por los escalares).

DEFINICIÓN. El sub-espacio del espacio vectorial $\mathcal{V}$ con el conjunto de base $L(\mathbf{a}_1,\ldots,\mathbf{a}_n)$ es se denota $L(\mathbf{a}_1,\ldots,\mathbf{a}_n)$ y se denomina *sub-espacio* extendido sobre los vectores $\mathbf{a}_1,\ldots,\mathbf{a}_n$ o sub-espacio generado por los vectores $\mathbf{a}_1,\ldots,\mathbf{a}_n$.
DEFINICIÓN. Se llama *envoltura lineal del conjunto* $\mathrm{M},\mathrm{M}\subset V$ la colección $L(\mathrm{M})$ de todas las combinaciones lineales de vectores de M con coeficientes en F. Se llama *envoltura lineal de un conjunto vacío el conjunto*$\{\mathbf{0}\}$.

La envoltura lineal del conjunto M es cerrado en $\mathcal{V}$.

DEFINICIÓN. Un sub-espacio del espacio $\mathcal{V}$ con conjunto de base $L(\mathrm{M})$se denota $L(\mathrm{M})$ y llamada *sub-espacio extendido sobre el conjunto* M o *sub-espacio generado por el conjunto* M.

Suma de sub-espacios. Sea $\mathcal{U}_1,\ldots,\mathcal{U}_m$de los sub-espacios del espacio vectorial $\mathcal{V}$ y $\mathbb{U}_1,\ldots,\mathbb{U}_m$sus conjuntos de base. El conjunto

$\{\mathbf{a}_1+\cdots+\mathbf{a}_m|\mathbf{a}_1\in\mathbb{U}_1,\ldots,\mathbf{a}_m\in\mathbb{U}_m\}$

se denota $\mathbb{U}_1+\cdots+\mathbb{U}_m$. se verifica sin duda que este conjunto es cerrado en el espacio $\mathcal{V}$.

DEFINICIÓN. Un sub-espacio del espacio $\mathcal{V}$ con conjunto de base $\mathbb{U}_1+\cdots+\mathbb{U}_m$ se denomina *suma de los sub-espacio* $\mathcal{U}_1,\ldots,\mathcal{U}_m$y se denota $\mathcal{U}_1+\cdots+\mathcal{U}_m$.

Nótese las propiedades siguientes de una suma de sub-espacios que se deducen sin duda de su definición.

PROPIEDAD 2.4. Si $\mathcal{L}$ y $\mathcal{U}$ son sub-espacios del espacio vectorial $\mathcal{V}$, entonces $\mathcal{U}+\mathcal{L}=\mathcal{L}+\mathcal{U}$.

PROPIEDAD 2.5. Si $\mathcal{L},\mathcal{U},\mathcal{W}$ son sub-espacios del espacio vectorial $\mathcal{V}$, entonces $\mathcal{L}+(\mathcal{U}+\mathcal{W})=(\mathcal{L}+\mathcal{U})+\mathcal{W}$.

PROPIEDAD 2.6. Si $\mathcal{L}$ es un sub-espacio del espacio $\mathcal{U}$, entonces $\mathcal{L}+\mathcal{U}=\mathcal{U}$.

Sean $\mathcal{L}_1,\ldots,\mathcal{L}_m$sub-espacios del espacio vectorial $\mathcal{V}$.

DEFINICIÓN. La suma $\mathcal{L}_1+\cdots+\mathcal{L}_m$ se denomina *suma directa de los sub-espacios* $\mathcal{L}_1,\ldots,\mathcal{L}_m$y se denota $\mathcal{L}_1\oplus\ldots\oplus\mathcal{L}_m$ si cualquier vector $\mathbf{a}$de $L_1+\cdots+L_m$se representa de manera única bajo la forma

$\mathbf{a}=\mathbf{a}_1+\cdots+\mathbf{a}_m$, donde $\mathbf{a}_1\in L_1,\ldots,\mathbf{a}_m\in L_m$.

En otros términos, la suma $\mathcal{L}_1+\cdots+\mathcal{L}_m$ se denomina *directa* si la igualdad $\mathbf{a}_1+\cdots+\mathbf{a}_m=\mathbf{b}_1+\cdots+\mathbf{b}_m$ implica las igualdades$\mathbf{a}_1=\mathbf{b}_1,\ldots,\mathbf{a}_m=\mathbf{b}_m$para todos $\mathbf{a}_1\mathbf{b}_1$ de $L_1,\ldots,\mathbf{a}_m,\mathbf{b}_m$ de L_m.

TEOREMA 2.1. *La suma de los sub-espacios* $\mathcal{L}$ *y* $\mathcal{U}$ *del espacio vectorial es directa si y solo si* $L\cap\mathbb{U}=\{\mathbf{0}\}$.

Demostración. Supóngase que $\mathcal{L}+\mathcal{U}=\mathcal{L}\oplus\mathcal{U}$. Entonces, para cualquier elemento $\mathbf{c}$de $L\cap\mathbb{U}$ se verifica la igualdad $\mathbf{c}+\mathbf{0}=\mathbf{0}+\mathbf{c}$, de la cual se deduce la igualdad $\mathbf{c}=\mathbf{0}$, ya que la suma $\mathcal{L}+\mathcal{U}$ es directa. Así, $L\cap\mathbb{U}=\{\mathbf{0}\}$.
Supóngase ahora que $L\cap\mathbb{U}=\{\mathbf{0}\}$. Para todos los vectores $\mathbf{a}_1$, $\mathbf{b}_1$ de $\mathcal{L}$ y $\mathbf{a}_2$, $\mathbf{b}_2$de $\mathbb{U}$ la igualdad $\mathbf{a}_1+\mathbf{a}_2=\mathbf{b}_1+\mathbf{b}_2$ implica las relaciones $\mathbf{a}_1-\mathbf{b}_1=\mathbf{a}_2-\mathbf{b}_2\in L\cap\mathbb{U}=\{\mathbf{0}\}$, por consiguiente,$\mathbf{a}_1=\mathbf{b}_1$y $\mathbf{a}_2=\mathbf{b}_2$. Por tanto, la suma $\mathcal{L}+\mathcal{U}$ es directa.□

TEOREMA 2.2. *La suma de los sub-espacios* $\mathcal{L}_1,\ldots,\mathcal{L}_m$ *del espacio vectorial es una suma directa si para todos los vectores* $\mathbf{a}_1$ *de* $\mathcal{L}_1,\ldots,\mathbf{a}_m$*de* $\mathcal{L}_m$ *la igualdad*

(1) $\mathbf{a}_1+\cdots+\mathbf{a}_m=\mathbf{0}$

Implica las igualdades

(2) $\mathbf{a}_1=\mathbf{0},\ldots,\mathbf{a}_m=\mathbf{0}$.

Demostración. Supóngase que la suma $\mathcal{L}_1 + \cdots + \mathcal{L}_m$es directa. Entonces de la igualdad (1), que se puede escribir bajo la forma $\mathbf{a}_1 + \cdots + \mathbf{a}_m = \mathbf{0} + \cdots + \mathbf{0}$resultan, las igualdades$\mathbf{a}_1 = \mathbf{0}, \ldots, \mathbf{a}_m = \mathbf{0}$.

Admítase ahora que para todos los vectores $\mathbf{a}_1, \ldots, \mathbf{a}_m$respectivamente de $\mathcal{L}_1, \ldots, \mathcal{L}_m$, la igualdad (1) implica las igualdades (2).Cualesquiera que sean los vectores $\mathbf{b}_1\mathbf{c}_1$ de $\mathcal{L}_1, \ldots, \mathbf{b}_m, \mathbb{c}_m$ de $\mathcal{L}_m$ la igualdad

(3) $\mathbf{b}_1 + \cdots + \mathbf{b}_m = \mathbf{c}_1 + \cdots + \mathbf{c}_m$

Implica $(\mathbf{b}_1 - \mathbf{c}_1) + \cdots + (\mathbf{b}_m - \mathbf{c}_m) = \mathbf{0}$, de donde, por la hipótesis, resultan, las igualdades

$\mathbf{b}_1 - \mathbf{c}_1 = \mathbf{0}, \ldots, \mathbf{b}_m - \mathbf{c}_m = \mathbf{0}$.

Así, de (3) resultan, las igualdades

$\mathbf{b}_1 = \mathbf{c}_1, \ldots, \mathbf{b}_m = \mathbf{c}_m$.

Por tanto, la suma $\mathcal{L}_1 + \cdots + \mathcal{L}_m$ es directa. □

Variedades lineales. Sean $\mathcal{L}$ un sub-espacio del espacio vectorial $\mathcal{V}$ y L su conjunto de base. Defínase sobre el conjunto V la relación binaria $\sim$ imponiendo que $a \sim b$ si y solo si $\mathbf{a} - \mathbf{b} \in L$. Llámese esta relación binaria de *congruencia* en $\mathcal{L}$.

PROPOSICION 2.3. *Una congruencia sobre el conjunto V en $\mathcal{L}$ es una relación de equivalencia sobre V.*

Demostración. La congruencia en $\mathcal{L}$ es al parecer reflexiva. La relación en $\mathcal{L}$ es simétrica, ya que de $\mathbf{a} - \mathbf{b} \in L$ se deduce $\mathbf{b} - \mathbf{a} \in L$. La congruencia en $\mathcal{L}$ es transitiva, ya que para todos $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$ de $\mathbf{a} - \mathbf{b} \in L$ y $\mathbf{b} - \mathbf{c} \in L$ se deduce$\mathbf{a} - \mathbf{c} = (\mathbf{a} - \mathbf{b}) + (\mathbf{b} - \mathbf{c}) \in L$. Por tanto, la congruencia en $\mathcal{L}$ es una relación de equivalencia sobre el conjunto V. □

La relación de equivalencia $\sim$ sobre V define la partición del conjunto V en clases de equivalencia.

DEFINICIÓN. Sea $\mathcal{L}$ un sub-espacio del espacio vectorial $\mathcal{V}$. Cualquier clase d equivalencia de la congruencia en $\mathcal{L}$ se denomina *variedad linaria del espacio $\mathcal{V}$ de dirección $\mathcal{L}$*.

EJEMPLO. El conjunto de todas las soluciones de un sistema compatible de ecuaciones lineales en n variables es una variedad lineal de dirección $\mathcal{L}$ de un espacio vectorial aritmético en n dimensiones, donde $\mathcal{L}$ es el espacio de las soluciones del sistema de ecuaciones homogéneas correspondiente.

De la definición dada anteriormente se derivan las propiedades 2.7 y 2.8.

PROPIEDAD 2.7. *Dos vectores del espacio vectorial $\mathcal{V}$ pertenecen, a una misma variedad lineal de dirección $\mathcal{L}$ si y solo si su diferencia pertenece, a L.*

PROPIEDAD 2.8. *Las dos variedades lineales del espacio vectorial $\mathcal{V}$ de dirección $\mathcal{L}$ son ya sea iguales o disjuntas. La reunión de todas las variedades lineales del espacio $\mathcal{V}$ de dirección $\mathcal{L}$ es igual al conjunto V.*

Nótese $\mathbf{a} + L(\mathbf{a} \in V)$ el conjunto $\{\mathbf{a} + \mathbb{x} | \mathbb{x} \in L\}$.

PROPIEDAD 2.9. *Si H es una variedad lineal del espacio vectorial $\mathcal{V}$ de dirección $\mathcal{L}$ y$\mathbf{a} \in H$, entonces $H = \mathbf{a} + L$.*

Demostración. Dado que todo elemento del conjunto $\mathbf{a} + L$ es comparable a $\mathbf{a}$en $\mathcal{L}$, se tiene $\mathbf{a} + L \subset H$. Además, todo elemento $\mathbf{c}$ de H es comparable a $\mathbf{a}$en L, y se tiene $\mathbf{c} - \mathbf{a} \in L$ y $\mathbb{c} \in \mathbf{a} + L$. Así, $H \subset \mathbf{a} + L$. Por tanto, $H = \mathbf{a} + L$. □

Corolario 2.4. *Si$\mathbf{a}$y $\mathbf{b}$son elementos de una misma variedad lineales del espacio $\mathcal{V}$ de dirección $\mathcal{L}$, entonces se tiene $\mathbf{a} + L = \mathbf{b} + L$.*

Corolario 2.5. *Si* $\mathcal{L}$ $\mathcal{V}$ *y* $\mathbf{c}$ *un elemento cualquiera del espacio* $\mathcal{V}$, $\mathbf{c}+L$ *es entonces una variedad lineal del espacio* $\mathcal{V}$ *de dirección* $\mathcal{L}$.

PROPIEDAD 2.10. *Sean* $\mathcal{L}$ *y* $\mathcal{U}$ *sub-espacios del espacio vectorial* $\mathcal{V}$ *y* $\mathbf{a},\mathbf{b}\in V$. *La inclusión* $\mathbf{a}+L\subset\mathbf{b}+\mathbb{U}$ *tiene lugar si y solo si* $\mathbf{a}-\mathbf{b}\in\mathbb{U}$ y $L\subset\mathbb{U}$.

Demostración. Supóngase que $\mathbf{a}+L\subset\mathbf{b}+\mathbb{U}$. Entonces, $\mathbf{a}\in\mathbf{b}+\mathbb{U}$, $\mathbf{a}-\mathbf{b}\in\mathbb{U}$ y $\mathbf{a}+\mathbb{U}=\mathbf{b}+\mathbb{U}$, así, $\mathbf{a}+L\subset\mathbf{a}+\mathbb{U}$ y $L\subset\mathbb{U}$.

Admítase ahora que se satisfacen las condiciones $\mathbf{a}-\mathbf{b}\in\mathbb{U}, L\subset\mathbb{U}$. Entonces, $\mathbf{a}+\mathbb{U}=\mathbf{b}+\mathbb{U}$ y $\mathbf{a}+L\subset\mathbf{a}+\mathbb{U}$; así, $\mathbf{a}+L\subset\mathbf{b}+\mathbb{U}$. □

PROPIEDAD 2.11. *Una intersección de variedades lineales* $\mathbf{a}+L$ *y* $\mathbf{b}+\mathbb{U}$ *de un espacio vectorial no es vacío si y solo si* $\mathbf{a}-\mathbf{b}\in L+\mathbb{U}$.

Demostración. Supóngase que la intersección $\mathbb{a}+L\cap\mathbf{b}+\mathbb{U}$ no está vacía y $\mathbf{c}$es un elemento de la intercesión. Entonces, $\mathbb{c}=\mathbf{a}+\mathbb{I}=\mathbf{b}+\mathbb{u}$, donde $\mathbb{I}\in L$ y $\mathbb{u}\in\mathbb{U}$; así $\mathbf{a}-\mathbf{b}=-\mathbb{I}+\mathbb{u}$ y $\mathbf{a}-\mathbf{b}\in L+\mathbb{U}$.

Admítase ahora que $\mathbf{a}-\mathbf{b}\in L+\mathbb{U}$. entonces se tiene $\mathbf{a}-\mathbf{b}=\mathbb{v}+\mathbb{u}$, donde $\mathbb{v}\in L,\mathbb{u}\in\mathbb{U}$ y $\mathbf{a}+(-\mathbb{v})=\mathbf{b}+\mathbb{u}$. Por tanto, las variedades $\mathbf{a}+L$ y $\mathbf{b}+\mathbb{U}$ tienen un elemento común $\mathbf{b}+\mathbb{u}$. □

PROPIEDAD 2.12. *Si la intersección de la variedad lineal de dirección* $\mathcal{L}$ *y de la variedad lineal de dirección* $\mathcal{U}$ *no está vacía, ella constituye entonces una variedad lineal de dirección* $\mathcal{L}\cap\mathcal{U}$.

Demostración. Supóngase que la intersección de las variedades $\mathbf{a}+L$ y $\mathbf{b}+\mathbb{U}$ no esta vacío y que $\mathbf{c}$ es su elemento común; en este caso $\mathbf{a}+L=\mathbf{c}+L,\mathbf{b}+\mathbb{U}=\mathbf{c}+\mathbb{U}$ y $\mathbf{a}+L\cap\mathbf{b}+\mathbb{U}=\mathbf{c}+L\cap\mathbf{c}+\mathbb{U}$. se verifica sin duda que $\mathbf{c}+L\cap\mathbf{c}+\mathbb{U}=\mathbf{c}+(L\cap\mathbb{U})$. Así, $\mathbf{a}+L\cap\mathbf{b}+\mathbb{U}=\mathbf{c}(L\cap\mathbb{U})$, es decir que la intersección de dos variedades lineales es una variedad lineal de dirección $\mathcal{L}\cap\mathcal{U}$. □

PROPIEDAD 2.13. *Si un espacio vectorial* $\mathcal{V}$ *es una suma directa de los sub-espacios* $\mathcal{L}$ *y* $\mathcal{U}$, *la intersección de las variedades lineales de dirección* $\mathcal{L}$ *y de dirección* $\mathcal{U}$ *solo consta de un elemento.*

Demostración. Sea $\mathcal{V}=\mathcal{L}\oplus\mathcal{U}$, entonces $V=L+\mathbb{U}, L\cap\mathbb{U}=\{\mathbf{0}\}$. Sean $\mathbf{a}+L$ y $\mathbf{b}+\mathbb{U}$ variedades lineales de direcciones $\mathcal{L}$ y $\mathcal{U}$ respectivamente. Según la propiedad 2.11, su intersección no está vacía, ya que $\mathbf{a}-\mathbf{b}\in V=L+\mathbb{U}$. Sea $\mathbf{c}$ el elemento común de la intersección. Según la propiedad 2.12, se deduce que $\mathbf{a}+L\cap\mathbf{b}+\mathbb{U}=\mathbf{c}+(L\cap\mathbb{U})=\mathbf{c}+\{\mathbf{0}\}=\mathbf{c}$. □

Ejercicios

1. Cada una de las condiciones siguientes se desprende del espacio vectorial $\mathcal{V}=\mathcal{F}^n$de los conjuntos de vectores $(x_1,\dots,x_n)$. ¿cuáles de estos conjuntos están cerrados en $\mathcal{V}$ respecto a la adición y multiplicación por los escalares:

(a) $x_1+x_2+\cdots+x_n=\mathbf{0}$;
(b) $x_1+x_2+\cdots+x_n=1$;
(c) $x_1-x_2-\cdots-x_n=\mathbf{0}$;
(d) $x_n=\mathbf{0}$;
(e) $x_1=1$;
(f) $x_1=x_n=\mathbf{0}$;
(g) $x_1\cdot x_n=\mathbf{0}$;
(h) $x_1=x_2=\cdots=x_n$?

2. Sea $\mathcal{V}=\mathcal{F}^{n\times n}$el espacio vectorial de todas las matrices $n\times n$ sobre un cuerpo. Mostrar que el conjunto de todas las matrices simétricas (simétricas izquierdas) del espacio $\mathcal{V}$ es un sub-espacio del espacio $\mathcal{V}$ con respecto a la adición y multiplicación por escalares.

3. Sean $\mathcal{V}=\mathcal{F}^{n\times n}$sobre el cuerpo numérico $\mathcal{F}$, $\mathcal{L}$ un sub-espacio de toda matriz $n\times n$ simétrica y $\mathcal{U}$ un sub-espacio de toda matriz simétrica izquierda. Demostrar que $\mathcal{V}=\mathcal{L}\oplus\mathcal{U}$.

4. Sea $\mathcal{V}$ un espacio vectorial (sobre $\mathcal{R}$) de todas las funciones $\mathfrak{f}$ tres veces derivables: $\mathbb{R} \to \mathbb{R}$ que satisfacen a la condición $\mathfrak{f}'' + \mathfrak{f}' = \mathbf{0}$.Demostrar que el conjunto de todas las funciones del espacio, que satisfacen a la condición $\mathfrak{f}'' + \mathfrak{f} = \mathbf{0}$, constituye un sub-espacio del espacio $\mathcal{V}$.

5. Sea $\mathcal{V} = \mathcal{R}^{2\times 2}$ un espacio vectorial de las matrices 2×2 sobre el cuerpo $\mathcal{R}$ de números reales. Mostrar que el conjunto de todas las matrices sobre $\mathcal{R}$ del aspecto $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ constituye un sub-espacio del espacio $\mathcal{V}$.

6. Sean $\mathbf{a}_1, \dots, \mathbf{a}_k, \mathbf{b}_1, \dots, \mathbf{b}_s$ vectores del espacio vectorial $\mathcal{V}$. Demostrar que $\mathcal{L}(\mathbf{a}_1, \dots, \mathbf{a}_k) + \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_s) = \mathcal{L}(\mathbf{a}_1, \dots, \mathbf{a}_k, \mathbf{b}_1, \dots, \mathbf{b}_s)$.

7. Demostrar que la intersección de cualquier conjunto de sub-espacios del espacio vectorial $\mathcal{V}$ es un sub-espacio del espacio $\mathcal{V}$.

8. Sean $\mathcal{L}$ y $\mathcal{U}$ sub-espacios del espacio vectorial $\mathcal{V}$. Demostrar que $\mathcal{L} + \mathcal{U}$ es una intersección de todos los sub-espacios del espacio $\mathcal{V}$ que contiene los sub-espacios $\mathcal{L}$ y $\mathcal{U}$.

9. Sean $\mathbf{a}, \mathbf{b}, \mathbf{c}$ vectores que satisfacen a la condición $\mathbf{a} + \lambda\mathbf{b} + \xi\mathbf{c} = 0$ donde λ, ξ son escalares no nulos. Demostrar que $\mathcal{L}(\mathbf{a}, \mathbf{b}) = \mathcal{L}(\mathbf{b}, \mathbf{c}) = \mathcal{L}(\mathbf{c}, \mathbf{a})$.

10. Supóngase que los vectores $\mathbf{a}, \mathbf{b}$son linealmente independientes. Demostrar que $\mathcal{L}(\mathbf{a}, \mathbf{b}) = \mathcal{L}(\mathbf{a}) \oplus \mathcal{L}(\mathbf{b}) \oplus \mathcal{L}(\mathbf{c})$.

11. Sea un sistema de vectores $\mathbf{a}, \mathbf{b}, \mathbf{c}$ linealmente independiente. Demostrar que $\mathcal{L}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \mathcal{L}(\mathbf{a}) \oplus \mathcal{L}(\mathbf{b}) \oplus \mathcal{L}(\mathbf{c})$.

12. Demostrar que si el vector $\mathbf{b}$ es una combinación lineal de los vectores $\mathbf{a}_1, \dots, \mathbf{a}_m$, entonces $\mathcal{L}(\mathbf{a}_1, \dots, \mathbf{a}_m,) = \mathcal{L}(\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b})$.

13. Supóngase que el espacio vectorial $\mathcal{V}$ es generado por el sub-espacio $\mathcal{U}$ y el vector $\mathbf{a}$.Demostrar que si $\mathbf{b} \in \mathbf{V} \setminus \mathbb{U}$,entonces $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}(\mathbf{b})$.

14. Sea $\mathcal{V}$ la suma de los sub-espacios $\mathcal{L}$ y $\mathcal{U}$. Demostrar que $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$ si se puede representar de manera única al menos un vector $\mathbf{c} \in \mathcal{V}$ bajo la forma de $\mathbf{c} = \mathbf{a} + \mathbf{b}$,donde $\mathbf{a} \in \mathbf{L}, \mathbf{b} \in \mathbb{U}$.

15. Sea $\mathcal{V}$ una suma directa de los sub-espacios $\mathcal{L}$ y $\mathcal{U}$. Demostrar que $\mathbf{a}_1, \dots, \mathbf{a}_m$ es un sistema linealmente independiente de vectores del sub-espacio $\mathcal{L}$, y $\mathbf{b}_1, \dots, \mathbf{b}_s$ un sistema linealmente independiente de vectores de $\mathcal{U}$, entonces $\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b}_1, \dots, \mathbf{b}_s$ es un sistema linealmente independiente de vectores del espacio $\mathcal{V}$.

16. Sea $\mathcal{V}$ un espacio vectorial, suma de los sub-espacios $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$. Demostrar que $\mathcal{V} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$ si y solo si $\mathcal{L}_1 \cap \mathcal{L}_2 = \mathbf{0}$ y $(\mathcal{L}_1 + \mathcal{L}_2) \cap \mathcal{L}_3 = \mathbf{0}$.

17. Sean $\mathcal{V} = \mathcal{F}^n$, donde $\mathcal{F}$ es un cuerpo de los escalares compuestos de dos elementos, y $\mathbf{b}_1, \dots, \mathbf{b}_m$un sistema independiente de vectores del espacio $\mathcal{V}$. ¿De cuántos vectores consta la envoltura lineal $\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_m)$, de esos vectores?

§ 3. Base y dimensión del espacio vectorial

Base del espacio vectorial. Sea $\mathcal{V}$ un espacio vectorial con el conjunto de base V. Si existe en V un conjunto finito $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$de vectores tales como $V = L(\mathbf{a}_1, \dots, \mathbf{a}_m)$, se dice entonces que el espacio $\mathcal{V}$ es generado por el conjunto finito $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$que se llamara *conjunto* (o sistema) que *genera los espacios* $\mathcal{V}$.

DEFINICIÓN. Un espacio vectorial se denomina *dimensión finita* si es generado por un conjunto finito de vectores.

DFINICIÓN. Se llama *base de un espacio de vectores de dimensión finita* a un sistema de vectores no vacío, finito y linealmente independiente que genera este espacio.

EJEMPLO. Sea $\mathcal{V} = \mathcal{F}^n$un espacio vectorial aritmético sobre el cuerpo $\mathcal{F}$. El sistema de los vectores de unidad $\mathbf{e_1} = (\mathbf{1}, \mathbf{0}, \dots, \mathbf{0}), \dots, \mathbf{e_n} = (\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \mathbf{1})$ es linealmente independiente y genera el espacio $\mathcal{V}$, es decir $V = L(\mathbf{e_1}, \dots, \mathbf{e_n})$. Por tanto, el sistema de vectores $\mathbf{e_1}, \dots, \mathbf{e_n}$constituye la base del espacio $\mathcal{F}^n$.

TEOREMA 3.1. *Cualquier espacio vectorial* $\neq \{\mathbf{0}\}$*y de dimensión finita posee una base. Además, si el sistema de los vectores* $(1)\mathbf{a}_1, \dots, \mathbf{a}_m$ *genera el espacio vectorial* $\mathcal{V}$, *entonces la base del sistema de los vectores* (1) *es la base del espacio* $\mathcal{V}$.

Demostración. Supóngase que el espacio $\mathcal{V}$ se genero por el sistema de vectores (1), es decir $V = L(\mathbf{a}_1, \dots, \mathbf{a}_m)$; se puede estimar que los vectores del sistema (1)no son nulos. Según el TEOREMA 5.1, el sistema (1) tiene una base. Sea

$(2)\mathbf{b}_1, \dots, \mathbf{b}_n$

la base del sistema(1). El sistema (2) entonces también genera el espacio $\mathcal{V}$, es decir $V = L(\mathbf{b}_1, \dots, \mathbf{b}_n)$. Además, el sistema (2) es linealmente independiente. Por tanto, el sistema (2) es la base del sistema (1) y que parte, de la base del espacio $\mathcal{V}$. □

TEOREMA. 3.2. *Sea $\mathcal{V}$ un espacio vectorial $\neq \{\mathbf{0}\}$y de dimensión finita. Entonces, el número de elementos de una base del espacio $\mathcal{V}$ vale el número de cualquier otra base de este espacio.*

Demostración. Según el TEOREMA 3.1, el espacio $\mathcal{V}$ posee una base. Sean

$(1)\mathbf{b}_1, \dots, \mathbf{b}_n$

una base del espacio $\mathcal{V}$ y

$(2)\mathbf{c_1}, \dots, \mathbf{c_s}$

cualquier otra base de este espacio. Entonces, $V = L(\mathbf{b}_1, \dots, \mathbf{b}_n) = L(\mathbf{c_1}, \dots, \mathbf{c_s})$. Los sistemas de vectores (1) y (2) son equivalentes. Así, según el TEOREMA 5.1.2, $n = s$. □

COROLARIO 3.3. *Si la base del espacio vectorial $\mathcal{V}$ está compuesta de n elementos, entonces, para $\mathcal{K} > n$ cualquier sistema de vectores del espacio $\mathcal{V}$ es linealmente dependiente.*

Demostración. Si $\mathbf{b}_1, \dots, \mathbf{b}_n$es una base del espacio $\mathcal{V}$ y $\mathbf{a}_1, \dots, \mathbf{a}_k$de los vectores cualquieras de V, entonces $\mathbf{a}_1, \dots, \mathbf{a}_k \in L(\mathbf{b}_1, \dots, \mathbf{b}_n)$. Se deduce, según el TEOREMA 5.1, por $\mathcal{K} > n$, que el sistema de vectores $\mathbf{a}_1, \dots, \mathbf{a}_k$es linealmente dependiente.□

COROLARIO 3.4. *Si la base del espacio vectorial $\mathcal{V}$ consta de n vectores, entonces cualquier sistema de n vectores que genera el espacio $\mathcal{V}$ es una base de este espacio.*

TEOREMA3.5. *Cualquier sub-espacio $\mathcal{U}$ de un espacio vectorial de dimensión finita $\mathcal{V}$ es de dimensión finita. Si $\mathcal{V}$ posee una base compuesta de n elementos y $\mathcal{U}$ es un sub-espacio $\neq \{\mathbf{0}\}$, entonces $\mathcal{U}$ posee una base cuyo número de elementos es inferior o igual a n.*

Demostración. Sean $\mathcal{V}$ un espacio vectorial de dimensión finita y $\mathcal{U}$ su sub-espacio. Si $\mathcal{U}$ es un sub-espacio $= \{\mathbf{0}\}$, entonces es de dimensión finita. Supóngase que el sub-espacio $\mathcal{U}$ es $\neq \{\mathbf{0}\}$. Entonces $\mathcal{V}$ es un espacio $\neq \{\mathbf{0}\}$ y según el TEOREMA 3.1, posee una base. Supóngase que la base del espacio $\mathcal{V}$ consta de n elementos. Entonces, cualquier sistema de vectores linealmente independiente del espacio $\mathcal{V}$ contiene n elementos o más

Sea $\mathbf{u}_1$un elemento no nulo del espacio $\mathcal{U}$. Si es $\mathbb{U} \neq L(\mathbf{u}_1)$, existe un vector $\mathbf{u}_2 \in \mathbb{U} - L(\mathbf{u}_1)$, el sistema de los vectores $\mathbf{u}_1, \mathbf{u}_2$ es linealmente independiente. Si es $\mathbb{U} \neq L(\mathbf{u}_1, \mathbf{u}_2)$, existe un vector $\mathbf{u}_3 \in \mathbb{U} \setminus L(\mathbf{u}_1, \mathbf{u}_2)$, el sistema de vectores $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$es linealmente independiente. Continuando de este modo, se llega a la sucesión

$(1)\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \dots$

de los elementos linealmente independientes del espacio $\mathcal{U}$. Esta sucesión consta de n elementos o más. Existe así un número natural $m \leq n (m > 0)$tal como $\mathbb{U} = L(\mathbf{u}_1, \dots, \mathbf{u}_m)$. El sub-espacio $\mathcal{U}$ es así de dimensión finita y el sistema de vectores $\mathbf{u}_1, \dots, \mathbf{u}_m$es su base.□

Completar hasta la base de un sistema de vectores independientes. ¿Es posible incluir en cualquier base un sistema cualquiera de vectores linealmente independiente?

TEOREMA 3.6. *Un sistema de vectores linealmente independiente del espacio vectorial $\mathcal{V}$ de dimensión finita y $\neq \{0\}$que no constituye una base del espacio se puede completar hasta la base del espacio $\mathcal{V}$.*

Demostración. Sea

$(1)\mathbf{a}_1, \dots, \mathbf{a}_m$

Un sistema linealmente independiente que no constituye una base del espacio $\mathcal{V}$. Sea $\mathbf{b}_1, \dots, \mathbf{b}_n$la base del espacio $\mathcal{V}$. Considérese el sistema

$(\mathbf{S})\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b}_1, \dots, \mathbf{b}_n$.

Según el corolario 3.3, este sistema es linealmente dependiente. Así, al menos uno de los vectores $\mathbf{b}_1, \dots, \mathbf{b}_n$es una combinacion lineal de vectores que le preceden, en el sistema $(\mathbf{S})$. elimínese uno de esos vectores del sistema $(\mathbf{S})$; se obtienen el sistema

$(\mathbf{S_1})\ \mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b}_1^{(1)}, \dots, \mathbf{b}_{n-1}^{(1)}$,

equivalen al sistema $(\mathbf{S})$y, por tanto, generador del espacio $\mathcal{V}$. Si $(\mathbf{S_1})$ consta de más n elementos, entonces, (según el corolario 3.3) es linealmente dependiente y que parte de uno de los elementos $\mathbf{b}_1^{(1)}, \dots, \mathbf{b}_{n-1}^{(1)}$ es una combinación lineal de los elementos preceden. Suprímase este elemento de $(\mathbf{S_1})$. Entonces se obtiene que el sistema $(\mathbf{S_2})$ equivalen al sistema $(\mathbf{S})$y por tanto, es generador del espacio $\mathcal{V}$. Mediante la operación después de m eliminaciones se llega a la sucesión al sistema de vectores

$(\mathbf{S_m})\ \mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b}_1^{(m)}, \dots, \mathbf{b}_{n-m}^{(m)}$,

equivalen al sistema $(\mathbf{S})$y así generan el espacio $\mathcal{V}$. Según el corolario 3.4 el sistema $(\mathbf{S_m})$ es la base del espacio $\mathcal{V}$. Como el sistema $(\mathbf{S_m})$ contiene el sistema de partida (1), el sistema $(\mathbf{S_m})$ es la base buscada del espacio $\mathcal{V}$. □

TEOREMA 3.7. *Si $\mathcal{U}$es un sub-espacio del espacio vectorial $\mathcal{V}$ de dimensión finita, entonces existe un sub-espacio $\mathcal{W}$ del espacio $\mathcal{V}$, tal como*

$(1)\ \mathcal{V} = \mathcal{U} \oplus \mathcal{W}$ •

Demostración. La igualdad (1)se cumple si $\mathcal{U}$ es un sub-espacio trivial, es decir un sub-espacio $= \{\mathbf{0}\}$o un sub-espacio que coincide con $\mathcal{V}$. Supóngase que $\mathcal{U}$ es un sub-espacio no trivial y

$(2)\mathbf{a}_1, \dots, \mathbf{a}_m$

es su base. Según el TEOREMA 3.6 el sistema (2) se puede completar hasta la base del espacio $\mathcal{V}$, es decir que existen vectores $\mathbf{a}_{m+1}, \dots, \mathbf{a}_n$ para los cuales el sistema

$(3)\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{a}_{m+1}, \dots, \mathbf{a}_n$

se convierte en la base del espacio $\mathcal{V}$. Entonces,

$(4)\ V = \mathbb{U} + \mathbb{W}$,

donde $\mathbb{W} = L(\mathbf{a}_{m+1}, \dots, \mathbf{a}_n)$. Demuéstrese que

$(5)\ \mathbb{U} \cap \mathbb{W} = \{\mathbf{0}\}$.

De hecho, si $\mathbf{c} \in \mathbb{U} + \mathbb{W}$, entonces

$\mathbf{c} = \boldsymbol{\alpha_1}\mathbf{a_1} + \cdots + \boldsymbol{\alpha_m}\mathbf{a_m} \in \mathbb{U}, \mathbf{c} = \boldsymbol{\alpha}_{m+1}\mathbf{a}_{m+1} + \cdots + \boldsymbol{\alpha}_n\mathbf{a}_n \in \mathbb{W}$

Y por tanto,

$\boldsymbol{\alpha_1}\mathbf{a_1} + \cdots + \boldsymbol{\alpha_m}\mathbf{a_m} + (-\boldsymbol{\alpha}_{m+1})\mathbf{a}_{m+1} + \cdots + (-\boldsymbol{\alpha}_n)\mathbf{a}_n = \mathbf{0}$.

Conforme a la independencia lineal del sistema (3), todos los coeficientes se anulan y en particular, $\alpha_1 = 0, \dots, \alpha_m = 0$. Por tanto, $\mathbf{c} = \mathbf{0}$, es decir (5) se verifica.

Sobre la base de (4)y (5) se concluye que para $\mathcal{W} = \mathcal{L}(\mathbf{a}_{m+1}, \dots, \mathbf{a}_n)$ se tiene la igualdad (1). □

COROLARIO 3.8. Si el sistema (3) es la base del espacio $\mathcal{V}$, entonces

$\mathcal{V} = \mathcal{L}(\mathbf{a}_1, \dots, \mathbf{a}_m) \oplus \mathcal{L}(\mathbf{a}_{m+1}, \dots, \mathbf{a}_n)$.

Dimensión del espacio vectorial. Uno de los más importantes invariantes del espacio vectorial es su dimensión.

DEFINICIÓN. Se llama *dimensión del espacio vectorial de dimensión finita* $\neq \{\mathbf{0}\}$ el número de vectores de una base cualquiera de espacio. La dimensión del espacio vectorial $= \{0\}$es por convención igual a cero. La dimensión del espacio vectorial diseñada por dim $\mathcal{V}$.

Ejemplo. Sea $\mathcal{F}^n$un espacio vectorial aritmético sobre el cuerpo $\mathcal{F}$. Los vectores $\mathbf{e_1}(1,0,\dots,0), \mathbf{e_1} = (0,1,0,\dots,0), \dots, \mathbf{e_n} = (0,0,\dots,0,1)$ constituyen la base del espacio. Por tanto, dim $\mathcal{F}^n = n$.

Considérese algunas propiedades de la dimensión.

PROIEDAD 3.1. Si $\mathcal{V}$ es un espacio vectorial de dimensión finita y dim $\mathcal{V} = n$, entonces, para $\mathcal{K} > n$, cualquier sistema de $\mathcal{K}$ vectores del espacio $\mathcal{V}$ es linealmente dependiente.

Demostración. Si $n = 0$, entonces $\mathcal{V} = \{\mathbf{0}\}$y la propiedad 3.1 es verificada. Pero si dim$\mathcal{K} = n > 0$, la base del espacio $\mathcal{V}$ es entonces constituida por n vectores. Según la propiedad 3.3, se deduce que para $\mathcal{K} > n$ cualquier sistema de $\mathcal{K}$ vectores del espacio $\mathcal{V}$ es linealmente dependiente. □

COROLARIO 3.9. *Si dim* $\mathcal{V} = n$ *y el sistema de vectores* $\boldsymbol{b_1}, \dots, \boldsymbol{b_m}$*del espacio* $\mathcal{V}$ *es linealmente independiente, entonces* $m \leq n$.

PROPIEDAD 3.2. *Si* $\mathcal{U}$*es un sub-espacio de un espacio vectorial de dimensión finita* $\mathcal{V}$, *entonces*

(1) dim $\mathcal{U} \leq$ dim $\mathcal{V}$.

Demostración. La desigualdad (1)es al parecer verdadera si $\mathcal{U} = \{\mathbf{0}\}$. pero si el sub-espacio es $\neq \{\mathbf{0}\}$, entonces (según el TEOREMA 3.5) es de dimensión finita y (según el TEOREMA 3.1) tiene una base. Sea $\mathbf{b_1}, \dots, \mathbf{b_m}$la base del sub-espacio $\mathcal{U}$. Entonces, dim $\mathcal{U} = m$. En el espacio $\mathcal{V}$ el sistema de vectores $\mathbf{b_1}, \dots, \mathbf{b_m}$es linealmente independiente. Así, según el corolario 3.9 $m \leq n$. □

PROPIEDAD 3.3 *Si* $\mathcal{U}$*es un sub-espacio del espacio vectorial de dimension finita y* dim $\mathcal{U} =$ dim $\mathcal{V}$,*entonces se tiene* $\mathcal{U} = \mathcal{V}$.

Demostración. Si el sub-espacio $\mathcal{U} = \{\mathbf{0}\}$, entonces dim $\mathcal{U} = 0$. Por tanto, conforme a la hipótesis dim $\mathcal{V} = 0$. Así $\mathcal{V}$ es igualmente un espacio vectorial igual a $\{\mathbf{0}\}$. Por tanto, $\mathcal{U} = \mathcal{V}$.

Supóngase que $\mathcal{U} \neq \{\mathbf{0}\}$. Entonces es igual que $\mathcal{V}$ de dimensión finita y, según el TEOREMA 3.1, posee una base. Sea $\mathbf{b_1}, \dots, \mathbf{b_n}$ su base. Entonces se tiene dim $\mathcal{U} = n$ y por hipótesis, dim $\mathcal{V} = n$. El sistema $\mathbf{b_1}, \dots, \mathbf{b_n}$es así igualmente una base del espacio $\mathcal{V}$. Por tanto, $\mathcal{U} = \mathcal{V}$. □

PROPIEDAD 3.4 *Si el espacio vectorial de dimensión finita* $\mathcal{V}$ *es una suma directa de los sub-espacios* $\mathcal{U}$ *y* $\mathcal{L}$, *entonces*

(1) dim $\mathcal{V} =$ dim $\mathcal{U} +$ dim $\mathcal{L}$.

Demostración. Por hipótesis $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}$ y, por tanto,

(2) $U \cap L = \{\mathbf{0}\}$,

(3) $V = U + L$.

Si $\mathcal{U}$ o $\mathcal{L}$ son iguales a $\{\mathbf{0}\}$, la igualdad (1) es al parecer verdadera.

Supóngase que $\mathcal{U}$ y $\mathcal{L}$ son $\neq \{\mathbf{0}\}$. Sean

$(4)\mathbf{b_1}, \dots, \mathbf{b_m}$,

$(5)\mathbf{b_{m+1}}, \dots, \mathbf{b_{m+s}}$,

las bases del espacio$\mathcal{U}$ y $\mathcal{L}$ respectivamente. Demuéstrese que el sistema

$(6)\mathbf{b_1}, \dots, \mathbf{b_m}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+s}}$

es una base del espacio$\mathcal{V}$. Conforme a (2), se tiene

(7) $L(\mathbf{b_1}, \dots, \mathbf{b_m}) \cap \boldsymbol{L}(\mathbf{b_{m+1}}, \dots, \mathbf{b_{m+s}}) = \{\mathbf{0}\}$.

El sistema (6) es linealmente independiente. De hecho, para cualquier escalar $\boldsymbol{\lambda_1}, \dots, \boldsymbol{\lambda_{m+s}}$de la igualdad

$\boldsymbol{\lambda_1}\mathbf{b_1} + \cdots + \boldsymbol{\lambda_m}\mathbf{b_m} + \boldsymbol{\lambda_{m+1}}\mathbf{b_{m+1}} + \cdots + \boldsymbol{\lambda_{m+s}}\mathbf{b_{m+s}} = \mathbf{0}$,

conforme a (7)resultan las igualdades

$(8)\boldsymbol{\lambda_1}\mathbf{b_1} + \cdots + \boldsymbol{\lambda_m}\mathbf{b_m} = 0, \boldsymbol{\lambda_{m+1}}\mathbf{b_{m+1}} + \cdots + \boldsymbol{\lambda_{m+s}}\mathbf{b_{m+s}} = \mathbf{0}$,

y como los sistemas (4)y (5) son linealmente independientes, se deduce de (8) que $\boldsymbol{\lambda_1 = 0, \dots, \lambda_m = 0, \dots, \lambda_{m+s} = 0}$. Además, conforme a (3),

$$V = \mathbb{U} + L = L(\mathbf{b_1}, \dots, \mathbf{b_m}) + \boldsymbol{L}(\mathbf{b_{m+1}}, \dots, \mathbf{b_{m+s}}) = L(\mathbf{b_1}, \dots, \mathbf{b_m}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+s}}),$$

Dicho de otro modo, el sistema(6) genera el espacio$\mathcal{V}$. En resumen, se demostró que el sistema (6)es una base del espacio $\mathcal{V}$. Por tanto, $\dim \mathcal{V} = m + s = \dim \mathcal{U} + \dim \mathcal{L}$. □

TEOREMA 3.10. *Si el espacio vectorial $\mathcal{V}$ es una suma de los sub-espacios de dimensión finita $\mathcal{U}$ y $\mathcal{L}$, entonces* $(1)\dim(\mathcal{U} + \mathcal{L}) + \dim(\mathcal{U} \cap \mathcal{L}) = \dim \mathcal{U} + \dim \mathcal{L}$.

Demostración. Supóngase que

$(2)\ \mathcal{V} = \mathcal{U} + \mathcal{L}$.

Si $U \cap L = \{0\}$, la suma (2) entonces es directa; así, según la propiedad 3.4, el TEOREMA es verdadero.□

Supóngase que $U \cap L \neq \emptyset$. Entonces el espacio $\mathcal{U} \cap \mathcal{L}$, al igual que $\mathcal{U}$, es de dimensión finita. Sea

$(2)\ \mathbf{b_1}, \dots, \mathbf{b_s}$

la base del espacio $\mathcal{U} \cap \mathcal{L}$. Complétesela hasta la base de los espacios $\mathcal{U}$ y $\mathcal{L}$. Sean

$(3)\mathbf{b_1}, \dots, \mathbf{b_s}, \mathbf{b_{s+1}}, \dots, \mathbf{b_m}$

La base del espacio $\mathcal{U}$ y

$(4)\mathbf{b_1}, \dots, \mathbf{b_s}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+k}}$

La base del espacio $\mathcal{L}$. Entonces,

$(5)\dim(\mathcal{U} + \mathcal{L}) = s, \dim \mathcal{U} = m, = \mathcal{S} + \mathcal{K}$

y, por tanto,

$(6)\mathbb{U} = L(\mathbf{b_1}, \dots, \mathbf{b_m}), \boldsymbol{L} = \boldsymbol{L}(\mathbf{b_1}, \dots, \mathbf{b_s}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+k}})$

De (4)y (6), se deriva que

$V = U + L = L(\mathbf{b_1}, \dots, \mathbf{b_m}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+k}})$,

es decir que el sistema

$(7)\mathbf{b_1}, \dots, \mathbf{b_m}, \mathbf{b_{m+1}}, \dots, \mathbf{b_{m+k}}$

genera el espacio $\mathcal{V}$.

Demuéstrese que el sistema (7)es linealmente independiente. Supóngase que se tiene

$(8)\boldsymbol{\lambda_1 \mathbf{b_1} + \dots + \lambda_s \mathbf{b_s} + \dots + \lambda_m \mathbf{b_m} + \lambda_{m+1} \mathbf{b_{m+1}} + \dots + \lambda_{m+k} \mathbf{b_{m+k}} = 0}$

De (6)y (8), se deriva que

$\boldsymbol{\lambda_{m+1} \mathbf{b_{m+1}} + \dots + \lambda_{m+k} \mathbf{b_{m+k}} \in \mathbb{U} \cap L}$

y, por consiguiente,

$\boldsymbol{\lambda_{m+1} \mathbf{b_{m+1}} + \dots + \lambda_{m+k} \mathbf{b_{m+k}} \in L(\mathbf{b_1}, \dots, \mathbf{b_s})}$.

Conforme a la independencia lineal del sistema (5), se deduce que

$(9)\boldsymbol{\lambda_{m+1} = 0, \dots, \lambda_{m+k} = 0}$.

A partir de (8)y (9)se deduce la igualdad

$\boldsymbol{\lambda_1 \mathbf{b_1} + \dots + \lambda_m \mathbf{b_m} = 0}$.

Dada la independencia lineal del sistema (3), se deriva la igualdad

$\boldsymbol{\lambda_1 = 0, \dots, \lambda_m = 0}$.

En resumen, se estableció que el sistema (7)es linealmente independiente. Así, el sistema (7) es la base del espacio y $(10)\dim(\mathcal{U} + \mathcal{L}) = m + k$.

Conforme a (5) y (10), se tiene

$\dim(\mathcal{U} + \mathcal{L}) + \dim(\mathcal{U} \cap \mathcal{L}) = m + \mathcal{K} + s = \dim \mathcal{U} + \dim \mathcal{L}$. □

Ejercicios

1. Demostrar que el sistema de vectores $(\alpha,\beta),(\gamma,\delta)$ de un espacio vectorial aritmético en dos dimensiones $\mathcal{V}$ es una base del espacio $\mathcal{V}$ si y solo si $\alpha\delta-\beta\gamma\neq 0$.
2. Demostrar que el sistema de vectores $(1,1,1),(0,1,1)(1,0,1)$ es una base del espacio $\mathcal{V}=\mathcal{F}^3$. Buscar las líneas de coordenadas de los vectores unitarios $\mathbf{e_1}=(1,0,0),\mathbf{e_2}=(0,1,0),\mathbf{e_3}=(0,0,1),$ respecto a esta base.
3. Demostrar que para los escalares α,β,γ cualquier sistema de vectores$(1,\alpha,\beta),(0,1,\gamma),(0,0,1)$es una base del espacio $\mathcal{V}=\mathcal{F}^3$.
4. Sea $\mathcal{F}$ un cuerpo numérico. ¿A qué condiciones debe satisfacer los escalares $\alpha,\beta,\gamma\in F$ para que el sistema de vectores $(1,\alpha,\alpha^2)(1,\beta,\beta^2)(1,\gamma,\gamma^2)$ sea una base del espacio $\mathcal{F}^3$?
5. ¿A qué condiciones debe satisfacer el escalar λ para que el sistema de vectores $(\lambda,1,0),(1,\lambda,1)(0,1,\lambda)$ sea una base del espacio $\mathcal{C}^3$; del espacio $\mathcal{Q}^3$?
6. Sea $\mathcal{V}$ un espacio vectorial que constituye una suma directa de los sub-espacios de dimensión finita $\mathcal{L}_1$ y $\mathcal{L}_2$. Demostrar que después de haber completado la base del sub-espacio $\mathcal{L}_2$ por la base del sub-espacio $\mathcal{L}_1$ se obtiene la base del espacio $\mathcal{V}$.
7. Sea $\mathcal{F}$ un cuerpo constituido de dos elementos. ¿Cuantas bases diferentes posee el espacio $\mathcal{F}^3$?
8. Sea $\mathcal{V}$ un espacio vectorial en n dimensiones. Demostrar que el sistema de vectores $\mathbf{a_1},\dots,\mathbf{a_n}$es una base del espacio $\mathcal{V}$ si y solo si $\mathcal{V}=\mathcal{L}(\mathbf{a_1},\dots,\mathbf{a_n})$.
9. Sea $\mathcal{V}=\mathcal{F}^{m\times n}$un espacio vectorial de las matrices $m\times n$ sobre el cuerpo $\mathcal{F}$.¿Cuál es su base y su dimensión?
10. Sea $\mathcal{V}$ un espacio vectorial de dimensión finita $\neq\{\mathbf{0}\}$. Demostrar que la dimensión del sub-espacio $\mathcal{L}(\mathbf{a_1},\dots,\mathbf{a_m})$extendido sobre los vectores dados $\mathrm{a}_1,\dots,\mathrm{a}_m$del espacio $\mathcal{V}$ es del rango de la matriz compuesta con las líneas de coordenadas de los vectores proyectados en una base cualquiera.
11. Demostrar que el sistema $\mathbf{a_1},\dots,\mathbf{a_n}$de los vectores no nulos del espacio vectorial en n dimensiones $\mathcal{V}$ solo es una base del espacio $\mathcal{V}$ si $\mathbf{a_k}\notin\mathbf{L}(\mathbf{a_1},\dots,\mathbf{a_{k-1}})$ para $k=2,3,\dots,n$.
12. Sean $\mathcal{F}$ un cuerpo finito compuesto de p elementos y $\mathcal{V}=\mathcal{F}^n$. ¿Cuántas bases distintas posee el espacio vectorial $\mathcal{V}$?
13. Sean $\mathbf{a_1},\dots,\mathbf{a_n}$una base del espacio vectorial $\mathcal{V}$ y k un entero positivo inferior en n. Demostrar que $\mathcal{V}=\boldsymbol{\mathcal{L}}(\mathbf{a_1},\dots,\mathbf{a_k})\oplus\boldsymbol{\mathcal{L}}(\mathbf{a_{k+1}},\dots,\mathbf{a_n})$.
14. Sea $\mathbf{e_1},\dots,\mathbf{e_n}$una base estándar del espacio vectorial $\mathcal{V}=\mathcal{F}^n$. Demostrar que el sistema de vectores $\mathbf{a_1},\dots,\mathbf{a_n}$del espacio $\mathcal{V}$ es una base del espacio $\mathcal{V}$ si solo si $\mathbf{e_1},\dots,\mathbf{e_n}\in L\ (\mathbf{a_1},\dots,\mathbf{a_n})$.
15. Demostrar que si la suma de las dimensiones de dos sub-espacios de un espacio en n dimensiones es superior a n, esos sub-espacios poseen entonces un vector no nulo común.
16. Demostrar que el espacio vectorial $\mathcal{V}$ solo posee dos sub-espacios si y solo si el espacio $\mathcal{V}$ está en una dimensión.
17. Demostrar que un espacio vectorial en dos dimensiones sobre un cuerpo numérico posee un conjunto infinito de sub-espacios en una dimensión distinta.
18. Sean $\mathcal{V}=\mathcal{U}\oplus\mathcal{L}$, donde $\mathcal{V}$ es un espacio en tres dimensiones, y $\mathcal{U},\mathcal{L}$ los sub-espacios $\{\neq 0\}$no idénticos a $\mathcal{V}$. Demostrar que uno de los sub-espacios $\mathcal{U},\mathcal{L}$ está en una dimensión, y el otro en dos dimensiones.
19. Sean $\mathcal{L}$ y $\mathcal{U}$ sub-espacios en una dimensión diferente de un sub-espacio vectorial bidimensional $\mathcal{V}$. Demostrar que $\mathcal{V}=\mathcal{L}\oplus\mathcal{U}$.
20. Sean $\mathcal{L}$ y $\mathcal{U}$ sub-espacios en dos dimensiones diferentes de un espacio vectorial tridimensional $\mathcal{V}$. Demostrar que $\mathcal{V}=\mathcal{L}+\mathcal{U}$ y $\mathcal{L}\cap\mathcal{U}$ es un sub-espacio unidimensional.
21. Sean $\mathcal{L}$ y $\mathcal{U}$ sub-espacios de un espacio vectorial en n dimensiones $\mathcal{V}$ cuyas dimensiones son k y s respectivamente. Demostrar que:
    (a) Si $L\cap V=\{0\}$y $k+s=n,$ entonces $\mathcal{V}=\mathcal{L}\oplus\mathcal{U}$;
    (b) Si $\mathcal{V}=\mathcal{L}+\mathcal{U}$ y $k+s=n,$ entonces $\mathcal{V}=\mathcal{L}\oplus\mathcal{U}$.

22. Demostrar que el espacio vectorial en n dimensiones se puede representar, por $n > 1$, bajo forma de una suma directa de n sub-espacios unidimensionales.

23. Sea $\mathbf{b_1}, \dots, \mathbf{b_n}$ la base del espacio vectorial $\mathcal{V}$. Demostrar que $\mathcal{V} = \mathcal{L}(\mathbf{b_1}) \oplus \dots \oplus \mathcal{L}(\mathbf{b_n})$.

24. Sea $\mathcal{V} = \mathcal{L}_1 + \mathcal{L}_2 + \mathcal{L}_3$, donde $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ son sub-espacios del espacio en n dimensiones $\mathcal{V}$ cuyas dimensiones son r, s, t respectivamente. Demostrar que $\mathcal{V} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$ si y solo si $r + s + t = n$.

§ 4. Isomorfismos de los espacios vectoriales

Línea de coordenadas de un vector respecto a una base dada.

Sea $\mathcal{V}$ un espacio vectorial sobre el cuerpo $\mathcal{F}$.

TEOREMA 4.1. *Sea*

$(1)\mathbf{b_1}, \dots, \mathbf{b_n}$

La base del espacio vectorial $\mathcal{V}$. *Para cada vector* $\boldsymbol{a}$ *de* V *existe en* F^n *un vector aritmético único* $\alpha_1, \dots, \alpha_n$ *tal como*

$(2)\mathbf{a} = \alpha_1\mathbf{b_1} + \dots + \alpha_n\mathbf{b_n}$.

Demostración. Dado que el sistema de vectores (1) genera el espacio V cualquier vector $\mathbf{a}$ de V se puede representar bajo forma de una combinación lineal de los vectores del sistema (1) tal como (2). Esta representación es única. De hecho, si

$$\mathbf{a} = \beta_1\mathbf{b_1} + \dots + \beta_n\mathbf{b_n}\beta_i \in F$$

es una representación cualquiera de $\mathbf{a}$ en forma de una combinación lineal de vectores (1), entonces

$$(\alpha_1\ \beta_1)\mathbf{b_1} + \dots + (\alpha_n\ \beta_n)\mathbf{b_n} = 0.$$

Conforme a la independencia lineal del sistema (1) se deducen las igualdades

$\alpha_1\ \beta_1 = 0, \dots, \alpha_n\ \beta_n = 0$ y $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$.

Por tanto, el vector $\mathbf{a}$ posee una representación única bajo forma de una combinación lineal de los vectores de la base (1). □

DEFINICIÓN. Sean $\mathbf{b_1}, \dots, \mathbf{b_m}$ una base fija del espacio $\mathcal{V}, \mathbf{a} \in V$ y $\mathbf{a} = \alpha_1\mathbf{b_1} + \dots + \alpha_n\mathbf{b_n}$, donde $\alpha_1, \dots, \alpha_n \in F$. los coeficientes $\alpha_1, \dots, \alpha_n$ se denominan *coordenadas del vector* $\mathbf{a}$ *relativamente en la base fija.* El vector $(\alpha_1, \dots, \alpha_n) \in F^m$ se denomina *línea de coordenadas, mientras que el vector* $\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix}$ se denomina *coordenadas del vector* $\mathbf{a}$ *relativamente en la base fija.*

Isomorfismo del espacio vectorial. Se llama *aplicación del espacio vectorial* $\mathcal{U}$ *en* $\mathcal{V}$ a la aplicación del conjunto $\mathbb{U}$ en V.

DEFINICIÓN. La aplicación del espacio vectorial $\mathcal{U}$ sobre el espacio vectorial $\mathcal{V}$ se denomina *isomorfismo* si ella es inyectiva y satisface a las condiciones de linealidad:

$$f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b}), \qquad f(\boldsymbol{\lambda}\mathbf{a}) = \lambda f(\mathbf{a})$$

para a, b cualquiera de U y cualquier λ de F. Los espacios vectoriales $\mathcal{U}$ y $\mathcal{V}$ se denominan *isomorfos* si está en presencia de un isomorfismo de $\mathcal{U}$ sobre $\mathcal{V}$.

En otras palabras, la aplicación f del espacio vectorial $\mathcal{U}$ y $\mathcal{V}$ se denominan isomorfismo si ella es inyectiva y respecto a las operaciones principales del espacio $\mathcal{U}$ considerado como un álgebra.

La notación $\mathcal{U} \cong \mathcal{V}$ significa que los espacios vectoriales $\mathcal{U}$ y $\mathcal{V}$ son isomorfos.

TEOREMA 4.2. *Sean $\mathcal{V}$ un espacio vectorial en n dimensiones sobre el cuerpo $\mathcal{F}$ y $n > 0$. El espacio $\mathcal{V}$ entonces es isomorfo en el espacio vectorial aritmético $\mathcal{F}^n$.*

Demostración. Sea

$(1)\mathbf{b_1}, \ldots, \mathbf{b_n}$

una base fija del espacio $\mathcal{V}$. Sea

f: V → f^n

La función que asocia a cada vector $\mathbf{a}$ de V su línea de coordenadas$f(\mathbf{a})$ relativamente a la base fija. Sea ($\boldsymbol{\gamma_1}$,….,$\boldsymbol{\gamma_n}$) un vector arbitrario de F^n.El vector $\boldsymbol{\gamma_1 b_1}+\ldots+\boldsymbol{\gamma_n b_n}$es su imagen anticipada en la función f. Por tanto, f es la función de V sobre F^n.

Además, según el TEOREMA 4.1, para todos **a, b** de V si$f(\mathbf{a}) = f(b)$, entonces $\mathbf{a} = \mathbf{b}$. Por tanto, f es una función inyectiva de V sobreF^n. La función f satisface a las condiciones de linealidad. En efecto,

$Si\ \mathbf{a} = \propto_1 \boldsymbol{b_1}+\ldots+\propto_n \boldsymbol{b}_n, \boldsymbol{b} = \beta_1 \boldsymbol{b_1}+\ldots+\beta_n \boldsymbol{b_n}$, entonces

$$\mathbf{a} + \boldsymbol{b} = (\propto_1 + \beta_1)\, \boldsymbol{b_1}+\ldots+(\propto_n + \beta_n)\, \boldsymbol{b}_n$$

Y

$$f(\mathbf{a} + \boldsymbol{b}) = (\propto_1 + \beta_1, \ldots, \propto_n + \beta_n) =$$
$$= (\propto_1, \ldots, \propto_n) + (\beta_1, \ldots, \beta_n) = f(\mathbf{a}) + f(\boldsymbol{b}).$$

Así que, si $\lambda \in F$, entonces $\lambda\mathbf{a} = (\lambda \propto_1) b_1 +\ldots+ (\lambda \propto_n) b_n$ y

$f(\lambda\mathbf{a}) = (\lambda \propto_1, \ldots \lambda \propto_n) = \lambda(\propto_1, \ldots, \propto_n) = \lambda f(\mathbf{a})$.

En resumen, f satisface a las condiciones de linealidad. Por consiguiente, la función f es un isomorfismo del espacio $\mathcal{V}$en el espacio $\mathcal{F}^n$.□

TEOREMA 4.3. *Sea $\mathcal{V}$ un espacio vectorial en n dimensiones sobre la estructura $\mathcal{F}$ con una base fija y $n > 0$. La función $f: V \rightarrow F^n$ que asocia a cada vector* **a** *de V su línea de coordenadas relativamente a la base fija constituye un isomorfismo del espacio $\mathcal{V}$sobre el espacio vectorial aritmética $\mathcal{F}^n$.*

Este TEOREMA se deduce directamente del TEOREMA 4.2 y de su Demostración.

COROLARIO 4.4. *Sea $\mathcal{V}$ un espacio vectorial de dimensión finita$\neq \{0\}$ cuya base es fija. Un sistema de vectores del espacio $\mathcal{V}$ es linealmente dependiente si y solo si el sistema de líneas (columnas) de coordenadas de estos vectores relativamente en la base fija es linealmente dependiente.*

COROLARIO 4.5. *Sea $\mathcal{V}$un espacio vectorial de dimensión finita con base fija. El rango de sistema de vectores $a_1, \ldots, a_m$ del espacio $\mathcal{V}$ es igual al de la matriz compuesta de líneas (columnas) de coordenadas de estos vectores relativamente de base fija.*

Estúdiese las propiedades de isomorfismos de espacios vectoriales.

PROPIEDAD 4.1. *Sif es un isomorfismo del espacio vectorial $\mathcal{U}$sobre $\mathcal{V}$ y g un isomorfismo del espacio $\mathcal{V}$ sobre $\mathcal{W}$, entonces su composición es un isomorfismo de $\mathcal{U}$ sobre $\mathcal{W}$.*

Demostración. Por hipótesis, g$f$es una función inyectiva de U sobre W. La función g$f$satisface a las condiciones de linealidad. En efecto, conforme a la linealidad de las funciones g y f.

Para todos $\boldsymbol{a}$, $\boldsymbol{b}$de$V$y todo λ de F, se tiene:

$$(gf)(a + b) = g(f(a) + f(b)) =$$
$$= g(f(a)) + g(f(b)) = (gf)(a) + (gf)(b),$$

$$(gf)(\lambda a) = g(f(\lambda a)) = g(\lambda f(a)) = \lambda g(f(a)) = \lambda(gf)(a).$$

Por lo tanto, gf es un isomorfismo de $\mathcal{U}$sobre $\mathcal{V}$.□

PROPIEDAD 4.2. *Si f es un isomorfismo del espacio vectorial $\mathcal{U}$ sobre el espacio vectorial $\mathcal{V}$, entonces f^{-1} es un isomorfismo de $\mathcal{V}$ sobre $\mathcal{U}$.*

Demostración. Siendo f una función inyectiva de $\mathcal{U}$sobre$\mathcal{V}$, f^{-1} es una función inyectiva de Vsobre U. Además f^{-1}cumple con las condiciones de linealidad. Efectivamente, conforme a la linealidad de la función *f* para todo a de Vy todo λ de F, resulta:

$f\left(f^{-1}(\mathbf{a}) + f^{-1}(b)\right) = f\left(f^{-1}(\mathbf{a})\right) + f\left(f^{-1}(b)\right) = \mathbf{a} + \mathbf{b}$,

$f\left(\lambda f^{-1}(\mathbf{a})\right) = f\lambda\left(f^{-1}(\mathbf{a})\right) = \lambda\mathbf{a}$,

de donde

$f^{-1}(\mathbf{a} + \mathbf{b}) = f^{-1}(\mathbf{a}) + f^{-1}(b), \quad f^{-1}(\lambda\mathbf{a}) = \lambda f^{-1}(\mathbf{a})$.

Por tanto f^{-1} es un isomorfismo de $\mathcal{V}$sobre $\mathcal{U}$.□

PROPIEDAD 4.3. La relaciòn de isomorfismo de un conjunto de espacios vectoriales cualquiera sobre la estructura $\mathcal{F}$ es una relación de equivalencia.

Demostración. La relación de isomorfismo es aparentemente reflexiva. En virtud de la propiedad 4.1 ella es transitiva. En virtud de la propiedad 4.2, la relación de isomorfismo es simetrica. Asi pues, la relación de isomorfismo es una relación de equivalencia .

PROPIEDAD 4.4. Sean

(1) $b_1, \ldots, b_n$

una base de el espacio vectorial $\mathcal{U}$ y f un isomorfismo de $\mathcal{U}$ sobre el espacio vectorial $\mathcal{V}$. El sistema de vectores $f(b_1), \ldots, f(b_n)$ *entonces es una base del espacio $\mathcal{V}$.*

Demostración. El sistema de vectores

(2) $f(b_1), \ldots, f(b_n)$

es linealmente independiente. Efectivamente, conforme a la linealidad de la función f para todos $\lambda_1, \ldots, \lambda_n$ de F de la igualdad

$$\lambda_1 f(b_1) + \ldots + \lambda_n f(b_n) = 0',$$

donde $0'$ es un vector cero del espacio $\mathcal{V}$, resultan las igualdades

$f(\lambda_1 b_1 + \ldots + \lambda_n b_n) = 0' = f(0)$.

Como la función f es inyectiva de la última igualdad se deduce que

(3) $\lambda_1 b_1 + \ldots + \lambda_n b_n = 0$.

El sistema (1) que es linealmente independiente, de (3) derivan las igualdades

$\lambda_1 = 0, \ldots, \lambda_n = 0$.

Ademas , el sistema (1) genera el espacio $\mathcal{V}$. Efectivamente, si $\boldsymbol{c} \in V$,entonces el vector $f^{-1}(\boldsymbol{c}) \in$ U y se puede representarlo bajo la forma

(4) $f^{-1}(c) = \gamma_1 b_1 + \ldots + \gamma_n b_n (\gamma_1, \ldots, \gamma_n \in F)$,

dado que el sistema (1) es la base del espacio $\mathcal{U}$. Conforme a la linealidad de la función f de (4) resultan las igualdades

$$c = f(\gamma_1 b_1 + \ldots + \gamma_n b_n) = \gamma_1 f(b_1) + \ldots + \gamma_n f(b_n).$$

Por tanto, el sistema (2) genera el espacio $\mathcal{V}$ y sirve de base.

TEOREMA 4.6. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales de dimensión finita sobre la estructura $\mathcal{F}$. Los espacios $\mathcal{U}$ y $\mathcal{V}$ son isomorfos si y sólo si sus dimensiones son identicas.

Demostración. Supóngase que $\mathcal{U} \cong \mathcal{V}$. Si uno de estos espacios es igual a $\{0\}$, el otro tambien será igual a $\{0\}$, es decir que $\dim \mathcal{U} = dim\, \mathcal{V} = 0$. Supóngase ahora que $\mathcal{U}$ y $\mathcal{V}$ son espacios $\neq \{0\}$. Entonces, conforme a la propiedad 4.4, el número del elementos de la base del espacio $\mathcal{U}$ es equivalente al de la base del espacio $\mathcal{V}$(las dimensiones de estos espacios son identicas).

Planteese que $\dim \mathcal{U} = dim\, \mathcal{V} = n$. Si $n = 0$ los espacios $\mathcal{U}, \mathcal{V} = \{0\}$ por tanto son isomorfos. Pero si $n > 0$ entonces, según el TEOREMA 4.2 $\mathcal{U} \cong \mathcal{F}^n$ $y\, \mathcal{F}^n \cong \mathcal{V}$ se deduce, conforme a la transitividad del isomorfismo, los espacios vectoriales $\mathcal{U}\ y\ \mathcal{V}$ son isomorfismo.□

Ejercicios:

1. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales de dimensión finita sobre laestructura $\mathcal{F}$.Mostrar que existe un monomorfismo del espacio $\mathcal{U}$ en $\mathcal{V}$ si y solo si $\dim \mathcal{U} \leq dim\, \mathcal{V}$.
2. Sean $\mathcal{U}$ y $\mathcal{V}$espacios vectoriales de dimensión finita sobre laestructura $\mathcal{F}$. Demostrar que existe un epimorfismo del espacio $\mathcal{U}$ sobre $\mathcal{V}$ si y solo si $\dim \mathcal{U} \geq dim\, \mathcal{V}$.
3. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales en n dimensiones sobre una estructura finita$\mathcal{F}$ compuesto por m elementos . ¿Qué cantidad de isomorfismos del espacio $\mathcal{U}$ se encuentran en el espacio $\mathcal{V}$?
4. Dar un ejemplo de espacio vectorial sobre la estructura $\mathcal{F}$ que no sea de dimensión finita .
5. Sea $\mathcal{W}$ un espacio vectorial sobre la estructura $\mathcal{F}$ de dimensión no finita. Mostrar que existe un monomorfismo en todo espacio vectorial de dimensión finita $\mathcal{V}$ sobre la estructura $\mathcal{F}$ del espacio $\mathcal{W}$.

§ 5. Espacios vectoriales en multiplicación escalar

Multiplicación escalar en un espacio vectorial. Sean $\mathcal{V}$ un espacio vectorial sobre la estructura $\mathcal{F}$,V el conjunto de base del espacio $\mathcal{V}$ yF el conjunto de base de la estructura $\mathcal{F}$ llamado *conjunto de escalare*.

DEFINICIÓN: Se llama *multiplicación escalar en el espacio* $\mathcal{V}$ a la funciónV × V→F que asocia a cada par de elementos $\mathrm{a}, \mathrm{b}\ de$ V un escalar denotado $\mathbf{a} \cdot \boldsymbol{b}$ que satisface las siguientes condiciones :

(1) $\mathbf{a} \cdot \mathbf{b} = \mathbf{b} \cdot \mathbf{a}$ para todos $\mathbf{a}, \mathbf{b}$ de **V** ;

(2) $(\alpha \mathrm{a} + \beta \mathrm{b}) \cdot \mathrm{c} = \alpha(\mathrm{a} \cdot \mathrm{c}) + \beta(\mathrm{b} \cdot \mathrm{c})$ para todos $\mathbf{a}, \mathbf{b}$ de V

Y α, β de f.

El escalar $\mathbf{a} \cdot \mathbf{b}$ se llama producto escalar de vectores **a** y **b.**

DEFINICIÓN: Una multiplicación escalar en el espacio $\mathcal{V}$ se llama no generada si $\mathbf{a}.\mathbf{a} \neq 0$ para todo vector **a** de V no nulo.

Una multiplicación escalar en el espacio $\mathcal{V}$ se llama nula si $\mathbf{a} \cdot \mathbf{b} = 0$ para todos $\mathbf{a}, \mathbf{b}$ de V.

PROPOSICIÓN 5.1. Si $\mathcal{V}$ *es un espacio vectorial de multiplicación escalar, entonces* $\mathrm{a} \cdot 0 = 0$ *para todo* a *de V.*

Demostración. Conforme la condición (2), $\mathbf{a} \cdot \mathbf{0} = \mathbf{a} \cdot (\mathbf{0} + \mathbf{0}) = \mathbf{a} \cdot \mathbf{0} + \mathbf{a} \cdot \mathbf{0}$ y como resultado $\mathbf{a} \cdot \mathbf{0} + \mathbf{a} \cdot \mathbf{0} = \mathbf{a} \cdot \mathbf{0} + \mathbf{0}$.

Conforme la regla de simplificación, se deduce que $\mathbf{a} \cdot \mathbf{0} = \mathbf{0}$.□

Obsérvese que en todo espacio vectorial de dimensión finita $\neq \{0\}$ la multiplicación escalar se puede introducir de distintas formas.

Sea $\mathcal{V}$ un espacio vectorial con multiplicación escalar

(3) $V \times V \rightarrow F$,

que satisface a las condiciones (1) , (2) de la definición. Si $\mathcal{L}$ es un sub-espacio del espacio $\mathcal{V}$ entonces la función (3) induce la función $L \times L \rightarrow F$ que del mismo modo satisface en L las condiciones (1),(2).

Así mismo el producto vectorial $\mathcal{L}$se puede considerar como un espacio vectorial con multiplicación escalar.

Sistema de vectores ortogonal. Sea $\mathcal{V}$ un espacio vectorial (sobre la estructura $\mathcal{F}$) con multiplicación escalar.

DEFINICIÓN: Los vectores $\mathbf{a}, \mathbf{b}$ de V se llaman *ortogonales* o *mutuamente ortogonales* si el producto escalar es nulo.

La notación $\mathbf{a} \perp \mathbf{b}$ se traduce como $\mathbf{a} \cdot \mathbf{b} = \mathbf{0}$.

DEFINICIÓN: Un sistema de vectores $\mathbf{a}_1, \ldots, \mathbf{a}_m$ del espacio $\mathcal{V}$ se llama *ortogonal* si son ortogonales entre ellos dos vectores cualquiera del sistema. Un sistema que comprende un solo vector no nulo se considera como ortogonal. Un sistema de vectores ortogonales que compone la base del espacio $\mathcal{V}$ se llama *base ortogonal del espacio.*

TEOREMA 5.2. Sea $\mathcal{V}$ un espacio vectorial de multiplicación escalar no generado. El sistema de vectores ortogonales no nulos del espacio $\mathcal{V}$ es linealmente independiente.

Demostración . Sea

(1) $\mathbf{a}_1, \ldots, \mathbf{a}_m$

Un sistema de vectores ortogonales no nulos del espacio $\mathcal{V}$. Muestrese que

Para todos los escalares $\lambda_1, \ldots, \lambda_m$ (de F) de la igualdad

(2)$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0$

Para todos los coeficientes se deduce la igualdad a cero de todos los coeficientes. Multiplíquese los dos elemtos de la igualdad (2) para los vectores $\mathbf{a}_k, \boldsymbol{k} \in \{1, \ldots, m\}$ y se obtiene.

$\lambda_1(a_1 a_k) + \ldots + \lambda_k(a_k a_k) + \ldots + \lambda_m(a_m a_k) = 0.$

Conforme la ortogonalidad del sistema (1), deducimos que la igualdad

(3) $\lambda_k(\mathbf{a}_k \cdot \mathbf{a}_k) = 0.$

Dado que por hipótesis, $\mathbf{a}_k \neq 0$ y la multiplicación escalar en $\mathcal{V}$ no se genera, se tiene $a_k a_k \neq 0$. Por lo tanto, (3) se deriba la igualdad

$\lambda_R = 0$ para $k = 1, \ldots, m.$

Por lo tanto, el sistema de vectores (1) es linealmente independiente. □

COROLARIO 5.3. Si $\mathcal{V}$ es un espacio vectorial en n dimensiones $\neq \{\mathbf{0}\}$ con multiplicación escalar no generada entonces cualquier sistema ortogonal del espacio n vectores no nulos, constituyen la base ortogonal del espacio $\mathcal{V}$.

Procedimiento de ortogonalisación. El principio del proceso de ortogonalisación resulta de la demostración del TEOREMA.

TEOREMA 5.4. Sea $\mathcal{V}$ un espacio vectorial de dimensión finita con multiplicación escalar no generada. Un sistema ortogonal de vectores no nulos que no constituyen una base del espacio, puede ser completado hasta la base ortogonal del espacio.

Demostración. Sea $\dim \mathcal{V} = n > 1$ y

(1) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$

Un sistema ortogonal de vectores no nulos del espacio $\mathcal{V}$ que no constituyen una base del espacio, es decir $m < n$. Según el TEOREMA 3.6, el sistema (1) se puede completar hasta la base. Sea

(2) $b_{1,\ \ldots,}b_m, c_{m+1}, \ \ldots, c_n$

La base del espacio $\mathcal{V}$. Plantéese

(3) $b_{m+1} = c_{m+1} - \lambda_1 b_1 - \ldots - \lambda_m b_m$

Y búsquese para cualquier valor escalar $\lambda_{1,\ \ldots,}\lambda_m$ el vector b_{m+1} es ortogonal en todos los vectores del sistema de partida (1), es decir satisface a las condiciones

(4) $b_{m+1}b_i = 0 \qquad (i = 1, \ \ldots, \ m).$

En virtud de (3) y de la ortogonalidad del sistema (1), estas condiciones se pueden escribir bajo la forma $c_{m+1}b_i - \lambda_i (b_i b_i) = 0.$

Dado que $b_i \neq 0$ y $\boldsymbol{b_i} \cdot \boldsymbol{b_i} \neq 0$, estas condiciones se escriben bajo la forma

$$\lambda_i = \frac{\boldsymbol{c_{m+1}b_i}}{\boldsymbol{b_i b_i}} \qquad (i = 1, \ \ldots, m).$$

Con esta elección de coeficientes λ_i en la igualdad (3), el vector $\boldsymbol{b_{m+1}}$ satisface a las condiciones (4), es decir es ortogonal a cada vector del sistema (1). Se deduce de (3) conforme a la independencia lineal del sistema $\boldsymbol{b_1}, \ \ldots, \boldsymbol{b_m}, \boldsymbol{b_{m+1}}$, que $\boldsymbol{b_{m+1}} \neq \boldsymbol{0}$. Por lo tanto, $b_1, \ \ldots, b_m, \ b_{m+1}$ es el sistema ortogonal de vectores no nulos. Si $m + 1 < n$, se obtiene de modo similar el vector no nulo b_{m+2} ortogonal a los vectores $b_1, \ \ldots, b_m, b_{m+1}$. Mediante este procedimiento llamado *procedimiento de ortogonalisación del sistema* (2) se llega al sistema ortogonal $b_1, \ldots, b_m, \ b_{m+1}, \ \ldots, b_n$

de los vectores no nulos del espacio $\mathcal{V}$. Según el corolario 5.3, este sistema es la base ortogonal del espacio $\mathcal{V}$ y como resultado constituye el suplementario buscado del sistema inicial (1) hasta la base ortogonal del espacio $\mathcal{V}$.

□

Se ve fácilmente que la función del proceso de ortogonalisación a un sistema linealmente dependiente de vectores no nulos conduce un sistema que contiene un vector nulo.

COROLARIO 5.5. cualquier espacio vectorial de dimensión finita $\neq \{0\}$ *con multiplicación escalar no generada dispone de una base ortogonal.*

Demostración. En efecto, según el TEOREMA 3.1, un espacio de dimensión finita $\neq \{0\}$ cuenta con una base. Sea

(1) $\mathrm{B}_{1,\ \ldots,\ } \mathrm{b}_n$

La base del espacio $\mathcal{V}$. Si se plantea que b_1 es el sistema ortogonal de partida y si se aplica al sistema (1) el proceso de ortogonalisación, se obtiene la base ortogonal del espacio $\mathcal{V}$.

Suplementario Ortogonal de un sub-espacio. Sea $\mathcal{V}$ un espacio vectorial con multiplicación escalar y $\mathrm{M} \subset \mathrm{V}$. Si el vector $\mathbf{a}$ de V es ortogonal a cada vector de M se le designa por el simbolo $\mathbf{a} \perp \mathrm{M}$. El simbolo $\mathrm{M}^{\perp}$ designa el conjunto de todos los elementos del espacio $\mathcal{V}$ ortogonales a M:

$\mathrm{M}^{\perp} = \{\mathrm{a} \in \mathrm{V} | \mathrm{a} \perp \mathrm{M}\}.$

Se verifica fácilmente que el conjunto $\mathrm{M}^{\perp}$ no es vacio y es cerrado en $\mathcal{V}$, es decir cerrado con respecto a la adición y multiplicación por escalares.

DEFINICIÓN. Un sub-espacio del espacio de $\mathcal{V}$ con conjunto de base $\mathrm{M}^{\perp}$ se llama ortogonal al conjunto M.

Si $\mathcal{L}$ es un sub-espacio del espacio $\mathcal{V}$, entonces el símbolo $\mathcal{L}^{\perp}$ designa el sub-espacio en conjunto de base $\mathcal{L}^{\perp}$

DEFINICIÓN. Un sub-espacio $\mathcal{L}^{\perp}$ se llama *ortogonal a $\mathcal{L}$ en el espacio $\mathcal{V}$ o suplementario ortogonal de $\mathcal{L}$ en el espacio $\mathcal{V}$*.

Ejemplo. Sea $\mathcal{V} = \mathcal{F}^n$ un espacio vectorial aritmético sobre la estructura $\mathcal{F}$ con multiplicación escalar estándar. Sea $\mathrm{M} = \{\mathrm{a}_{1,\ \ldots\ ,}\mathrm{a_m}\} \subset \mathrm{F}^n$ Y

$\mathrm{a}_1 = (\alpha_{11},\ldots,\propto_{1\mathrm{n}})\ ,\ \ldots\ ,\mathrm{a_m} = (\propto_{\mathrm{m1}},\ \ldots\ ,\propto_{\mathrm{mn}})\quad (\propto_{ik} \in \mathrm{F})$.o

Considérese un sistema homogéneo de ecuaciones lineales

$$\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0,$$

(1) $\quad \ldots\ldots\ldots\ldots$

$$\propto_{\mathrm{m1}} x_1 + \ldots + \propto_{\mathrm{mn}} x_n = 0$$

Sobre la estructura $\mathcal{F}$. Se constata fácilmente que el conjunto $\mathrm{M}^{\perp}$ coincide con el conjunto de todas las soluciones del sistema (1). Sea $\mathcal{L} = \mathcal{L}\ (\mathrm{a}_{1,\ \ldots\ ,}\mathrm{a_m})$ y $\mathrm{L} = \mathrm{L}(\mathrm{a}_{1,\ \ldots\ ,}\mathrm{a_m}) = \mathrm{L(M)}$. Se verifica fácilmente que cada vector ortogonal a M es ortogonal a toda combinación lineal de vectores $\mathbf{a}_{1,\ \ldots\ ,}\mathbf{a_m}$, es decir $\mathrm{M}^{\perp} \subset \mathrm{L}^{\perp}$. Inversamente cada vector de $\mathrm{L}^{\perp}$ es ortogonal a M, es decir $\mathrm{L}^{\perp} \subset \mathrm{M}^{\perp}$. Así $\mathrm{M}^{\perp} = \mathrm{L}^{\perp}$. Por lo tanto, el espacio de soluciones de sistema homogéneo de ecuaciones lineales (1) coincide con el espacio $\mathcal{L}^{\perp}$.

TEOREMA 5.6. Sea v un espacio vectorial con multiplicación escalar y $\mathcal{L}$ su sub-espacio de dimensión finita, en el cual el cuadrado escalar de cualquier vector no nulo es diferente a cero. Entonces tenemos que $\mathcal{V} = \mathcal{L} \oplus L^{\perp}$.

Demostración. Si $\mathcal{L}$ es un sub-espacio $= \{0\}$, aparentemente el TEOREMA es verdadero.
Supóngase que $\mathcal{L}$ es un espacio $\neq \{0\}$. Demuéstrese que

(1) $\quad \mathrm{L} \cap \mathrm{L}^{\perp} = \{0\}.$

En efecto, si $\mathrm{a} \in \mathrm{L} \cap \mathrm{L}^{\perp}$, entonces $\mathbf{a}.\mathbf{a} = 0$. Por hipótesis, $\mathbf{a}.\mathbf{a} \neq 0$ por $\mathbf{a} \neq \mathbf{0}$. Por tanto, para $\mathbf{a} \in L \cap L^{\perp}$, se deduce de $\mathbf{a}.\mathbf{a} = 0$ que $\mathbf{a} = 0$.

Demuéstrese enseguida que

(2) $\quad \mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}$.

Por hipótesis $\mathcal{L}$ es un espacio vectorial de dimensión finita$\neq \{0\}$ con multiplicación no generada. conforme al corolario 5.5,
$\mathcal{L}$ Es provisto de una base ortogonal. Sea

(3) $\quad b_{1,\ \ldots\ ,}b_m$

La base ortogonal del espacio$\mathcal{L}$. Es necesario mostrar que para todo vector $\mathbf{a}$ de L existen escalares $\lambda_{1,\ \ldots\ ,}\lambda_m$ y un vector $\boldsymbol{x}$ tales que

(4) $\quad \mathbf{a} = \boldsymbol{\lambda_1 b_1} + \ldots + \boldsymbol{\lambda_m b_m} + \boldsymbol{x}, \quad \boldsymbol{x} \in \mathrm{L}^{\perp}.$

Multiplíquese los dos miembros de la igualdad (4) escalarmente por el vector $\boldsymbol{b_i}$, se obtiene $\mathbf{a}.\mathbf{b_i} = \boldsymbol{\lambda_i}(\boldsymbol{b_i}.\boldsymbol{b_i})$. Puesto que $\boldsymbol{b_i}.\boldsymbol{b_i} \neq 0$, se deducen las igualdades

(5) $\quad \boldsymbol{\lambda_i} = \frac{\mathbf{a}.\mathbf{b_i}}{\boldsymbol{b_i}.\boldsymbol{b_i}} \qquad (\mathrm{i} = 1,\ \ldots\ ,\mathrm{m}).$

Con una selección de escalares λ_i el vector $\boldsymbol{x} = \mathbf{a} - \boldsymbol{\lambda_1 b_1} - \ldots - \boldsymbol{\lambda_m b_m}$ es ortogonal a cada vector de la base (3), ya que en virtud de (4) y (5),

$$xb_i = \mathrm{a}b_i - \lambda_i(b_i b_i) = 0 \qquad (\mathrm{i} = 1, \ldots, \mathrm{m}).$$

El vector $\boldsymbol{x}$ es por tanto ortogonal a cualquier combinación lineal de vectores $\boldsymbol{b_1}, \ldots, \boldsymbol{b_m}\ \boldsymbol{y}$, -+ por lo tanto ortogonal a L; así pues

(6) $\boldsymbol{x} = \mathbf{a} - \boldsymbol{\lambda_1 b_1} - \ldots - \boldsymbol{\lambda_m b_m} \in \boldsymbol{L^{\perp}}$.

Sobre la base de (4) y (6) se concluye que estamos en presencia de una descomposición directa de (2). □

COROLARIO 5.7. *Si $\mathcal{L}$ es un sub-espacio de dimensión finita del espacio vectorial $\mathcal{V}$ con multiplicación escalar no generada, entonces $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}$.*

COROLARIO 5.8. *Si $\mathcal{L}$ es un sub-espacio del espacio vectorial de dimensión finita $\mathcal{V}$ con multiplicación escalar no generada, entonces $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}$.*

TEOREMA 5.9. *Si $\mathcal{L}$ es un sub-espacio de un espacio vectorial de dimensión finita $\mathcal{V}$ Con multiplicación escalar no gradenerada, entonces $(\mathcal{L}^{\perp})^{\perp} = \mathcal{L}$.*

Se deja a opción del lector demostrar este TEOREMA.

Ejercicios

1. Sea $\mathbf{a}$ un vector no nulo del espacio vectorial $\mathcal{V} = \Re^3$ con multiplicación escalar estándar. ¿Cuál es la dimensión de sub-espacio del espacio de $\mathcal{V}$ ortogonal al vector $\mathbf{a}$?

2. Sea $\mathbf{a}, \mathbf{b}$ vectores linealmente independientes del espacio $\mathcal{V} = \Re^3$ con multiplicación escalar estándar. Buscar la dimensión del sub-espacio ortogonal a los vectores $\mathbf{a}$ y $\mathbf{b}$.

3. Sea $\mathcal{V} = Q^2$ un espacio vectorial bidimensional sobre la estructura de números racionales con multiplicación escalar estándar. Buscar en $\mathcal{V}$ el sub espacio $\neq \{0\}$en el cual el cuadrado escalar de todo vector es diferente de 1.

4. Sea $\mathcal{V}$ un espacio vectorial con multiplicación escalar no generada. Demostrar que si un vector no nulo $\mathbf{b}$ es ortogonal a los vectores $\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m}$ del espacio $\mathcal{V}$, entonces $\mathbf{b} \notin \mathbf{L}(\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m})$.

5. Sea $\mathcal{V}$ un espacio vectorial con multiplicación escalar no gradenerada. Sea $\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m}$ un sistema de vectores linealmente independiente del espacio $\mathcal{V}$. Demostrar que si un vector no nulo $\mathbf{b}$ es ortogonal a los a los vectores $\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m}$, el sistema $\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{m}, \mathbf{b}$ se le denomina linealmente independiente.

6. Sea $\mathcal{L}$ un sub-espacio $\neq \{0\}$de un espacio vectorial de dimensión finita $\mathcal{V}$ con multiplicación escalar no gradenerada. Sean $\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m}$ una base ortogonal del espacio $\mathcal{L}$ y $\mathrm{b}_1, \ldots, \mathrm{b}_s$ una base ortogonal del espacio $\mathcal{L}^{\perp}$. Demostrar que: $\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m}, \mathrm{b}_1, \ldots, \mathrm{b}_s$ es una base Ortogonal del espacio $\mathcal{V}$.

7. Sean$\mathcal{L}$,$\mathcal{U}$ sub espacios de un espacio vectorial de dimensión finita $\mathcal{V}$ con multiplicación escalar no gradenerada. Demostrar que:

(a) $(\mathcal{L}^{\perp})^{\perp} = \mathcal{L}$; (b) $(\mathcal{L} + \mathcal{U})^{\perp} = \mathcal{L}^{\perp} \cap \mathcal{U}^{\perp}$; (c) $(\mathcal{L} \cap \mathcal{U})^{\perp} = \mathcal{L}^{\perp} + \mathcal{U}^{\perp}$.

8. Sean$\mathcal{L}$, $\mathcal{U}$ sub espacios del espacio vectorial de dimensión finita $\mathcal{V}$ con multiplicación escalar no gradenerada, la dimensión de $\mathcal{L}$ es inferior a la de $\mathcal{U}$. Demostrar que en el espacio $\mathcal{U}$ se encuentra un vector no nulo ortogonal al sub espacio$\mathcal{L}$.

9. Sean $\mathcal{L}$, $\mathcal{U}$ sub espacios del espacio vectorial de dimensión finita $\mathcal{V}$ con multiplicación escalar no gradenerada. Demostrar que existe en $\mathcal{V}$ un vector no nulo ortogonal a los sub espacios $\mathcal{L}$ y $\mathcal{U}$ Si $\mathcal{L} + \mathcal{U} \neq \mathcal{V}$.

§ 6. Espacios vectoriales Euclidianos

Espacio Vectorial euclidiano. Sea $\mathcal{V}$ un espacio vectorial con multiplicación escalar sobre la estructura $\Re$ de números reales. Este espacio también es conocido como espacio vectorial real.

DEFINICIÓN. Un espacio vectorial sobre la estructura $\Re$ con multiplicación escalar definida positiva (es decir $\mathbf{a}.\mathbf{a} > \mathbf{0}$ para todo $\mathbf{a} \in \mathrm{V} \setminus \{0\}$) se llama espacio vectorial euclidiano.

TEOREMA 6.1. Un espacio vectorial aritmético sobre la estructura $\Re$ con multiplicación escalar estándar es euclidiano.

Demostración. Sean $\mathcal{V} = \Re^n$ un espacio vectorial aritmético con multiplicación escalar estándar y $\mathbf{a} = (\alpha_1, \ldots, \propto_{\mathrm{n}})$, $\mathbf{b} = (\beta_1, \ldots, \beta_n)$ vectores de este espacio. Según la definición de la multiplicación escalar estándar, $\mathbf{ab} = \alpha_1\beta_1 + \ldots + \propto_{\mathrm{n}} \beta_n$. Por lo tanto $\mathbf{aa} = \alpha_1^2 + \ldots + \alpha_n^2$**.** Y como $\alpha_1, \ldots, \propto_{\mathrm{n}}$ son números reales, tenemos $\mathbf{aa} > 0$ para todo vector $\mathbf{a}$ no nulo del espacio $\mathcal{V}$.□

DEFINICIÓN. Un espacio vectorial aritmético $\Re^n$con multiplicación escalar estandar se llama espacio euclidiano estandar a n dimensiones y notese $\mathcal{E}_n$

Ejemplo. Considérese el conjunto V de todas las funciones reales de una variable real x continuas sobre el intervalo$[0\ ,1]$. El conjunto V con relación a la adición y a la multiplicación por numeros reales es un espacio (de dimensión infinita) vectorial.

Sobre $\Re$. La formula $f\mathrm{g} = \int f(x)\mathrm{g}\,(x)dx$ define en V la multiplicación escalar. Se obtiene así un espacio vectorial euclidiano con multiplicación escalar.

Norma del vector. Sea $\mathcal{V}$ un espacio vectorial euclidiano.

DEFINICIÓN. Se llama *norma de vector del espacio euclidiano* a la raíz cuadrada aritmética del cuadrado escalar del vector.

La norma del vector se denota ‖ a ‖

Por definición, ‖ a ‖$= \sqrt{\mathbf{a}.\mathbf{a}}$. así pues, ‖ $\mathbf{a}$ ‖$^{\mathbf{2}} = \mathbf{a}.\mathbf{a}$.

DEFINICIÓN. El vector $\boldsymbol{a}$ se llama normado si ‖ a ‖$= 1$.

El siguiente TEOREMA manifiesta las propiedades fundamentales de la norma de un vector.

TEOREMA 6.2. Si a,b son vectores del espacio euclidiano y $\lambda \in R$, entonces

(1) ‖ a ‖≥ 0 con ‖ a ‖$= 0$ si y solo si a $= 0$;

(2) ‖ λa ‖$= |\lambda|$ ‖ a ‖;

(3) $|\mathrm{a} \cdot \mathrm{b}| \leq$‖ a ‖·‖ b ‖ (*desigualdad de Cauchy-Bouniakovski);*

(4) ‖ a ‖·‖ b ‖$\leq$‖ a ‖ +‖ b ‖ (*desigualdad del triángulo*).

Demostración. La multiplicación escalar en un espacio euclidiano es defindа positiva , es decir ‖ a ‖$= \sqrt{\mathbf{a}.\mathbf{a}.} > 0$

para $\mathbf{a} \neq \mathbf{0}$. Además , ‖ a ‖$= 0$ para $\mathbf{a} = \mathbf{0}$

Según la definición de la norma

$$\| \boldsymbol{\lambda}\mathbf{a} \| = \sqrt{(\boldsymbol{\lambda}\mathbf{a})(\boldsymbol{\lambda}\mathbf{a})} = \sqrt{\boldsymbol{\lambda}^{\mathbf{2}}(\mathbf{aa})} = |\boldsymbol{\lambda}|\sqrt{\mathbf{aa}} = |\boldsymbol{\lambda}| \cdot \| \mathbf{a} \|,$$

Dicho de otra manera, (2) se verifica .

La desigualdad (3) es verdadera si $\mathbf{a} = \mathbf{0}$ o $\mathbf{b} = \mathbf{0}$**.** Por ello se planteará que $\mathbf{a}$ y $\mathbf{b}$ son vectores no nulos. Para todos los números reales α y β tenemos la desigualdades

$$(\alpha\mathbf{a} - \beta\mathbf{b})(\alpha\mathbf{a} - \beta\mathbf{b}) \geq 0.$$

Si se abre el parentesis en el primer miembro de la desigualdad

$\alpha^2\mathbf{a}^2 - 2\alpha\beta\mathbf{ab} + \beta^2\mathbf{b}^{\mathbf{2}} \geq 0$ y si se plantea $\alpha =$‖ $\mathbf{b}$ ‖ y $\beta =$‖ $\mathbf{a}$ ‖,

Se convierte

$2\,(\|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|)^2 - 2\,\|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|\cdot\mathbf{ab} \geq 0,$

$\|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|\,(\|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\| - \mathbf{ab}) \geq 0.$

Puesto que $\mathbf{a} \neq 0$ y $\mathbf{b} \neq 0$, tenemos a $\|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\| \neq 0$ y como resultado

(5) $\mathbf{ab} \leq \|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|.$

substituyase en esta desigualdad $-\mathbf{a}$ a $\mathbf{a}$:

$-\mathbf{a}\cdot\mathbf{b} \leq \|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|.$

sobre la base de dos últimas desigualdades se concluye que está presente la desigualdad (3).

Para demostrar la desigualdad (4) basta con mostrar que
$\|\,\mathbf{a}\,\| + \|\,\mathbf{b}\,\|^2 \leq (\|\,\mathbf{a}\,\| + \|\,\mathbf{b}\,\|)^2$. Se constata facilmente que
$\|\,\mathbf{a}+\mathbf{b}\,\|^2 = (\mathbf{a}+\mathbf{b})(\mathbf{a}+\mathbf{b}) = \|\,\mathbf{a}\,\|^2 + \|\,\mathbf{b}\,\|^2 + 2\mathbf{ab}$; ya que

$\|\,\mathbf{a}+\mathbf{b}\,\|^2 = (\|\,\mathbf{a}\,\| + \|\,\mathbf{b}\,\|)^2 + 2(\mathbf{ab} - \|\,\mathbf{a}\,\|\cdot\|\,\mathbf{b}\,\|).$

En virtud de (5), el segundo término del segundo miembro de la última igualdad es inferior o igual a cero, ya que

$\|\,\mathbf{a}+\mathbf{b}\,\|^2 \leq (\|\,\mathbf{a}\,\| + \|\,\mathbf{b}\,\|)^2;$

De donde se deduce la desigualdad (4). □

Base ortonormal del espacio euclidiano. Una de las nociones principales de los espacios euclidianos es la de ser de base ortonormal.

DEFINICIÓN**.** El sistema de vectores $\mathbf{a_1}, \ldots, \mathbf{a_m}$ del espacio euclidiano se llama *ortonormal* si es ortogonal, cuando cada vector está normado. El sistema de vectores ortonormal que constituye la base del espacio, se llama *base ortonormal del espacio*.

TEOREMA 6.3. Un espacio vectorial euclidiano de dimensión finita $\neq \{\mathbf{0}\}$ *dispone de una base ortonormada*.

Demostración. Sea $\mathcal{V}$ un espacio euclidiano con n dimensiones, $n > 0$. Según el corolario 5.5, $\mathcal{V}$ posee una base ortogonal; sea

(1) $\mathbf{b_1}, \ldots, \mathbf{b_n}$

una base tal. Nórmese el sistema (1), es decir fórmese el sistema

$$\boldsymbol{e_1} = \|\,\mathbf{b_1}\,\|^{-1}\,\mathbf{b_1},\ \ldots,\ \boldsymbol{e_n} = \|\,\mathbf{b_n}\,\|^{-1}\,\mathbf{b_n}.$$

Se ve fácilmente que

$$\boldsymbol{e_i e_k} = \begin{cases} 1 \text{ si } i = k, \\ 0 \text{ si } i \neq k. \end{cases}$$

Por lo tanto, el sistema $\mathrm{e}_1, \ldots, \mathrm{e}_n$ es una base ortonormal del espacio $\mathcal{V}$. □

Véase algunas propiedades de una base ortonormal.

PROPIEDAD 6.1 Si $\mathcal{V}$ *es un espacio euclidiano con* n *dimensiones* $\neq \{\mathbf{0}\}$*, entonces todo sistema ortonormal de* n *vectores constituye una base ortonormal del espacio* $\mathcal{V}$.

Esta propiedad proviene directamente del corolario 5.3.

PROPIEDAD 6.2. un sistema ortonormal de vectores de un espacio euclidiano de dimensión finita $\neq \{\mathbf{0}\}$ *se puede completar hasta la base ortonormal del espacio.*

Demostración. Según el TEOREMA 5.4 un sistema ortonormal de vectores $\mathbf{b_1}, \ldots, \mathbf{b_m}$ que no constituye una base se puede completar hasta una base ortogonal

$$\mathbf{b_1}, \ldots, \mathbf{b_m}, \mathbf{b_{m+1}}, \ldots, \mathbf{b_n}$$

del espacio. Si se norman los vectores $\mathbf{b}_{m+1}, \ldots, \mathbf{b}_n$ de este sistema, es decir si se substituye $\| \mathbf{b}_i \|^{-1} \cdot \mathbf{b}_i$ a $\mathbf{b}_i$ para $i = m+1, \ldots, n$. Obtenemos una base ortogonal del espacio.□

PROPIEDAD 6.3. Si $\boldsymbol{e_1}, \ldots, \boldsymbol{e_n}$ es una base ortonormal de un espacio euclidiano y $\mathbf{a} = \alpha_1 \boldsymbol{e_1} + \ldots + \alpha_n \boldsymbol{e}_n$, $\boldsymbol{b} = \beta_1 e_1 + \ldots + \beta_n e_n$
Son los vectores del espacio, entonces

$\mathbf{ab} = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n$ Y $\| a \|^2 = \alpha_1^2 + \ldots + \alpha_n^2$.

Esta propiedad se deduce sin problema de la del bilinealidad de la multiplicación escalar.

PROPIEDAD 6.4. *Si $e_1, \ldots, e_n$ es una base ortonormal de un espacio euclidiano y $\boldsymbol{a} = \alpha_1 \boldsymbol{e}_1 + \ldots + \alpha_n e_n$. Entonces $\alpha_i = \boldsymbol{a e_i}$ para $i = 1, \ldots, n$, es decir que las coordenadas del vector $\boldsymbol{a}$ son sus proyecciones sobre los vectores de base*.

Demostración. La igualdad $\alpha_i = \mathbf{a}\boldsymbol{e_i}$ se obtiene de la igualdad $\mathbf{a} = \alpha_1 e_1 + \ldots + \alpha_n e_n$ después la multiplicación escalar por el vector $\boldsymbol{e}_i$. □

PROPIEDAD 6.5. Si $\mathcal{L}$ es un sub-espacio del espacio euclidiano de dimensión finita $\mathcal{V}$, entonces $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}$ y $\dim\mathcal{V} = \dim\mathcal{L} + \dim\mathcal{L}^{\perp}$.

Esta propiedad proviene directamente del corolario 5.8 y de la propiedad 3.4 ya que en un espacio euclidiano la multiplicación escalar es no generada.

Isomorfismos de espacios euclidianos. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios euclidianos.

DEFINICIÓN. La función f del espacio euclidiano $\mathcal{U}$ sobre $\mathcal{V}$ se le llama *isomorfismo* si este es inyectiva y satisface a las condiciones:

(1) $f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b})$;

(2) $f(\boldsymbol{\lambda}\mathbf{a}) = \lambda f(\mathbf{a})$;

(3) $\mathbf{ab} = f(\mathbf{a})\, f(\mathbf{b})$

Para todos **a, b** de V y todo escalar λ de **R.** Los espacios euclidianos se llaman *isomorfos* si hay un isomorfismo del espacio euclidiano $\mathcal{U}$ sobre $\mathcal{V}$.

La denotación $\mathcal{U} \cong \mathcal{V}$ significa que los espacios euclidianos $\mathcal{U}$ y $\mathcal{V}$ son isomorfos.

Véase las siguientes propiedades de isomorfismos.

PROPIEDAD 6.6. Una relación de isomorfismo sobre un conjunto en el que consta de espacios euclidianos es una relación de equivalencia.

Demostración. Se observa sin problema que la relación de isomorfismos es reflexiva.

Aprovéchese estas propiedades 4.2 y 4.3 de los isomorfismos de los espacios vectoriales. Si f es un isomorfismo del espacio euclidiano $\mathcal{U}$ sobre $\mathcal{V}$, entonces f^{-1} es biyectivo y satisface a las condiciones de linealidad. Entonces, dado que f satisface a la condición (3), para todos $\mathbf{a}, \mathbf{b}$ de $\mathcal{V}$ tenemos

$\mathbf{a}\boldsymbol{b} = (f f^{-1})(\mathbf{a})\,(f f^{-1})(\mathbf{b}) = f(f^{-1}(\mathrm{a}))\, f(f^{-1}(\mathbf{b})) = f^{-1}(\mathbf{a}) f^{-1}(\mathbf{b})$,

Es decir la función f^{-1} satisface igualmente con la condición (3). f^{-1} es así un isomorfismo del espacio euclidiano $\mathcal{V}$ sobre $\mathcal{U}$. Por consecuencia la relación de isomorfismo de los espacios euclidianos es simétrica.

Sean $\mathcal{U}, \mathcal{V}, \mathcal{W}$ espacios euclidianos. Si f es un isomorfismo de $\mathcal{U}$ sobre $\mathcal{V}$ y g un isomorfismo de $\mathcal{V}$ sobre $\mathcal{W}$, entonces, según la propiedad 4.1 de los isomorfismos de los espacios vectoriales, la composición gf es una función inyectiva de $\mathcal{U}$ sobre $\mathcal{V}$ que satisface a las condiciones de linealidad. Luego, dado que

$\mathbf{ab}=f(\mathbf{a})\,f(\mathbf{b})$, $\quad f(\mathbf{a})\,f(\mathbf{b})=\mathrm{g}(f(\mathbf{a}))\,\mathrm{g}(f(\mathbf{b}))$,

Se tiene

$\mathbf{ab}=(\mathrm{g}f)(\mathbf{a})\ (\mathrm{g}f)(\mathbf{b})$

Para todos a, b de U. gf Es por lo tanto un isomorfismo del espacio euclidiano $\mathcal{U}$ sobre $\mathcal{W}$. Por consiguiente, la relación de isomorfismo es transitiva. □

PROPIEDAD 6.7. Sean $\mathcal{U},\mathcal{V}$ espacios euclidianos y f un isomorfismo de $\mathcal{U}$ sobre $\mathcal{V}$.
Si $\boldsymbol{e}_1 \ldots \boldsymbol{e}_n$ es una base ortonormal del espacio $\mathcal{U}$, entonces el sistema $f(\mathrm{e}_1),\ldots,f(\mathrm{e}_n)$ es una base ortonormal del espacio $\mathcal{V}$.

Demostración. Como f es un isomorfismo, tenemos que $e_i\ e_k=f(\mathrm{e}_i)\,f(\mathrm{e}_k)$. Por lo tanto

$$f(\mathrm{e}_i)\,f(\mathrm{e}_k)=e_ie_k=\begin{cases}1 & \text{si } i=k,\\ 0 & \text{si } i\neq k.\end{cases}$$

El sistema $f(\mathrm{e}_1),\ \ldots f(\mathrm{e}_n)$ es así ortonormal, por otro parte según la propiedad 4.4 de los isomorfismos de los espacios vectoriales, el sistema $f(\mathrm{e}_1),\ \ldots f(\mathrm{e}_n)$ es la base del espacio $\mathcal{V}$. □

TEOREMA 6.4. Todo espacio euclidiano $\neq\{0\}$ de dimensión n es isomorfo a un espacio euclidiano de dimensión n estándar.

Demostración. Sean $\mathcal{V}$ un espacio euclidiano a n dimensiones y $\boldsymbol{e}_1, \ldots \boldsymbol{e}_n$ Su base ortonormal fija. Sea $\mathcal{E}_n$ un espacio euclidiano estándar a n dimensiones. Según el TEOREMA 4.3 la función f: $\mathcal{V}\longrightarrow\boldsymbol{\mathcal{R}}^n$ que asocia a cada vector $\boldsymbol{x}=\xi_1\boldsymbol{e}_1+\ldots+\boldsymbol{e}_n$ de $\mathcal{V}$ su línea de coordenadas $(\xi_1, \ldots \xi_n)$ Es inyectiva y satisface a las condiciones de linealidad. Además si $\boldsymbol{y}=\eta_1\boldsymbol{e}_1+\ldots+\eta_n e_n$, entonces

$\boldsymbol{xy}=\xi_1\eta_1+\ldots+\xi_n\eta_n=(\xi_1, \ldots,\xi_n)(\eta_1, \ldots \eta_n)=f(\boldsymbol{x})f(\boldsymbol{y})$.

Por lo tanto f es un isomorfismo del espacio euclidiano $\mathcal{V}$ sobre el espacio euclidiano estándar $\boldsymbol{\mathcal{E}_n}$. □

TEOREMA 6.5. Dos espacios euclidianos de dimensión finita son isomorfas si y solo si sus dimensiones son las mismas.

Demostración. Sean $\mathcal{U}\ y\ \mathcal{V}$ espacios euclidianos de dimensión finita. Si los espacios $\mathcal{U}\ y\ \mathcal{V}$ son isomorfos, entonces tenemos que según el TEOREMA 4.6, $dim\mathcal{U}=dim\mathcal{V}$

Admítase manteniendo que $dim\,\mathcal{U}=dim\mathcal{V}=n\ Si\ n=0$, los espacios $\mathcal{U}\ y\ \mathcal{V}$ son entonces $=\{0\}$ y por tanto son isomorfos. Pero si $n>0$, entonces según el TEOREMA 6.4 $\mathcal{U}\cong\boldsymbol{\mathcal{E}_n}\ y\ \boldsymbol{\mathcal{E}_n}\cong\mathcal{V}$ en virtud de la transitividad del isomorfismo, se deduce que los espacios euclidianos $\mathcal{U}\ y\ \mathcal{V}$ son isomorfos. □

Ejercicios:

1. Sean a, b vectores de un espacio euclidiano ortogonales entre ellos. Mostrar que $\|\mathbf{a}+\mathbf{b}\|^2=\|\mathbf{a}\|^2+\|\mathbf{b}\|^2$
2. Mostrar que para todos los vectores a, b del espacio euclidiano $\|\mathrm{a}+b\|^2+\|\mathrm{a}-b\|^2=2(\|\mathrm{a}+\|^2+\|b\|^2$
3. Sean a, b vectores del espacio euclidiano tales que $\|\mathrm{a}\|=\|\boldsymbol{b}\|$.

Demostrar que los vectores $\mathrm{a}-b$ y $\mathrm{a}+b$ son ortogonales entre ellos.

4. Demostrar que para todos los vectores a, b del espacio euclidiano $|\ \|\mathrm{a}\|-\|b\|\ |\leq\|\mathrm{a}\pm b\|$.
5. Sean a, b vectores no nulos del espacio euclidiano. Buscar el vector de la forma $\mathrm{a}+\lambda b$, o $\lambda\,\epsilon\,R$, que posee la norma más pequeña y demostrar que ese vector es ortogonal al vector **a**.
6. Sean a, b vectores linealmente independientes de un espacio euclidiano tridimensional $\mathcal{V}$. Demostrar que en el espacio $\mathcal{V}$ solo hay dos vectores de norma unitaria que sean ortogonales a los vectores a y b.

7. Sea $\mathcal{V} = Q^2$ un espacio vectorial bidimensional en la estructura de números racionales con multiplicación escalar estándar. Buscar en $\mathcal{V}$ un subespacio $\neq \{0\}$ en el que el cuadrado escalar de un vector cualquiera es diferente de 1.

8. Sean a, b vectores linealmente independientes del espacio euclidiano $\mathcal{V}$ en n dimensiones. Buscar la dimensión del sub espacio del espacio $\mathcal{V}$ ortogonal a los vectores a y b.

9. Sea $\mathcal{U}$ un sub espacio del espacio euclidiano $\mathcal{V}$ en n dimensiones y $\mathcal{U}^{\perp}$ su suplementario ortogonal. Sean $a_{1,\ .\ .\ .,}\ a_s$ una base ortonormal del espacio $\mathcal{U}$ y $\boldsymbol{b_1}, \ .\ .\ .,\boldsymbol{b}_{n-s}$ Una base ortonormal del espacio $\mathcal{U}^{\perp}$. Demostrar que $a_{1,\ .\ .\ .,}\ a_s b_{1,}\ .\ .\ .\ b_{n-s}$ Es una base ortonormal del espacio $\mathcal{V}$.

10. Sean $\mathbf{a}, \boldsymbol{b}$ vectores del espacio vectorial euclidiano. Demostrar que

$|\mathrm{a.\,b}| = \|\mathrm{a}\| . \|\mathrm{b}\|$ si y solo si los vectores $\mathbf{a}$ y $\boldsymbol{b}$ son linealmente dependientes.

11. Sean $\mathrm{a}_{1,\ .\ .\ .}\mathrm{a}_m$ un sistema ortonormal de vectores del espacio euclidiano $\mathcal{V}$ plantéese que para cada vector $\boldsymbol{c}$ del espacio $\mathcal{V}$ $\| \boldsymbol{c} \|^2 = (\mathbf{a_1}\boldsymbol{c})^2 + \ .\ .\ . + (\mathbf{a}_m\boldsymbol{c})^2$.

Demostrar que el sistema de vectores $\mathrm{a}_1\ .\ .\ ., \mathrm{a}_m$ es una base del espacio $\mathcal{V}$.

12. Sean $\mathcal{L}, \mathcal{U}$ sub espacios del espacio vectorial euclidiano de dimensión finita. Demostrar que:

(a) $(\mathcal{L}^{\perp})^{\perp} = \mathcal{L}$; (b) $(\mathcal{L} + \mathcal{U})^{\perp} = \mathcal{L}^{\perp} \cap \mathcal{U}^{\perp}$; (c) $(\mathcal{L} \cap \mathcal{U})^{\perp} = \mathcal{L}^{\perp} + \mathcal{U}^{\perp}$.

CAPITULO VIII
OPERADORES LINEALES

§ 1. Funciones lineales

Funciones y operadores lineales. Pásese al estudio de los homomorfismos de espacios vectoriales los cuales igualmente se conocen como funciones lineales.

DEFINICIÓN. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales sobre el cuerpo de $\mathcal{F}$.

Una función $f: \mathcal{U} \to \mathcal{V}$ es llamada función lineal u homomorfismo, si esta última satisface a las condiciones de linealidad, es decir, para todos $\mathbf{a}, \boldsymbol{b} \in V$ y todo $\lambda \in F$ estas satisfacen las condiciones.

$f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b}), \quad f(\lambda \mathrm{a}) = \lambda f(\mathbf{a})$.

Si una función lineal de $\mathcal{U}$ sobre $\mathcal{V}$ es inyectiva, entonces se le llama *isomorfismo u función isomorfa de* $\mathcal{U}$ *sobre* $\mathcal{V}$. Un conjunto de todas las funciones lineales (homomorfismo) del espacio $\mathcal{U}$ en el espacio $\mathcal{V}$se denotará Hom($\mathcal{U}, \mathcal{V}$) .

Una función lineal del espacio vectorial $\mathcal{V}$ en él mismo, se llama operador lineal del espacio $\mathcal{V}$. Un conjunto de todos los operadores lineales del espacio $\mathcal{V}$ se denota Hom $(\mathcal{V}, \mathcal{V})$.

Sea φ una función lineal del espacio vectorial $\mathcal{U}$ sobre el espacio vectorial $\mathcal{V}$. Entonces para todos los vectores $\mathrm{a}_{1,\ .\ .\ .,}\ \mathrm{a}_n$ de $\mathcal{U}$ y todos escalares $\lambda_{1,\ .\ .\ .,}\ \lambda_m \in F,$ setiene

(1) $\varphi(\lambda_1 \mathbf{a}_1 + \ .\ .\ . + \lambda_m \mathrm{a}_m) = \lambda_1\ \varphi(\mathrm{a}_1) + \ .\ .\ . + \lambda_m\ \varphi(\mathrm{a}_m)$.

La demostración se efectúa por recurrencia sobre m. Si $m = 1$, en virtud de la linealidad de la función φ, se obtiene $\varphi(\lambda_1 \mathbf{a}_1) = \lambda_1\, \varphi(\mathbf{a}_1)$.

Plantéese que la proposición es verdadera para $m - 1$ vectores. Entonces si se utiliza la igualdad.

$$\lambda_1 \mathbf{a_1} + \ .\ .\ . + \lambda_{m-1}\mathbf{a}_{m-1} + \lambda_m \mathbf{a}_m = (\lambda_1 \mathrm{a}_1 + \ .\ .\ . + \lambda_{m-1}\ \mathrm{a}_{m-1}) + \\ + \lambda_m\ \mathrm{a}_{m,}$$

Se cumplen

$$\varphi(\lambda_1 a_1 + \ldots + \lambda_m a_m) = \varphi(\lambda_1 a_1 + \ldots + \lambda_{m-1} a_{m-1}) + \varphi(\lambda_m a_m).$$

Según la hipotesis de recurrencia

$$\varphi(\lambda_1 a_1 + \ldots + \lambda_{m-1} a_{m-1}) = \lambda_1 \varphi(a_1) + \ldots + \lambda_{m-1} \varphi(a_{m-1}).$$

Por lo tanto, $\varphi(\lambda_m a_m) = \lambda_m \varphi(a_m)$. Por consecuencia, la igualdad (1) es verificada.□

Ejemplo. 1. Sea $\mathcal{V}$ un espacio vectorial. La función $\varepsilon: \mathcal{V} \to \mathcal{V}$que asocia a cada vector x de V del mismo vector, es decir $\varepsilon(x) = x$ es un operador lineal. Se llama operador identico o espacio unitario.

2. Sea $\mathcal{V}$ un es pacio vectorial en la estructura $\mathcal{F}$ y λ un elemento fijo de la estructura. La función $\lambda_\varepsilon = \mathcal{V} \to \mathcal{V}$ que asocia un vector x el vector λ_x es un operador lineal del espacio $\mathcal{V}$. Lo llamaremos operador homotetia de coeficienteλ. El operador de homotetia de coeficiente$\lambda = 0$ llamado operador cero. El operador de homotetia de coeficiente $\lambda = 1$es un operador identico.

3. Sea $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$. Todo elemento x de $\mathcal{V}$ estará representada de manera única bajo la forma de $x = l + u$, donde $\boldsymbol{l} \in L$ y $\boldsymbol{u} \in U$. La funciòn $\mathcal{V} \to \mathcal{V}$ que asocia al vector x su componente $\boldsymbol{l}$ en el término directo de $\mathcal{U}$ es un operador lineal del espacio $\mathcal{V}$. Lo llamaremos operador proyectivo.

4. Sea $\mathcal{V}$ un espacio vectorial (en $\Re$) de funciones reales a una variable x definida e indefinidamente derivables en el conjunto R de números reales. El operador $D: \mathcal{V} \to \mathcal{V}$ que asocia a cada elemento $f \in V$se cumple $\frac{\boldsymbol{df}}{\boldsymbol{dx}}$ es un operador lineal ya que cumple las condiciones de linealidad

$$D(f + g) = D(f) + D(g); D(\lambda f) = \lambda D(f)$$

Para todos $f, g \in V$ y todo $\lambda \in R$. Este operador se le conoce como operador de derivación.

5. Sea $\mathcal{V} = \mathcal{F}^n$ un espacio aritmético de vectores columnas de n dimensiones y A una matriz cuadrada $n \times n$ fija en la estructura $\mathcal{F}$.

La función del espacio $\mathcal{V}$ en el mismo que se asocia a cada vector $\times \in F^n$ el vector AX es un operador lineal del espacio $\mathcal{V}$.

TEOREMA 1.1 *Sea $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales sobre la estructura $\mathcal{F}$, $e_1, \ldots, e_n$ la base del espacio $\mathcal{U}$ y $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ de los vectores arbitrarios del espacio $\mathcal{V}$. Existe una función lineal unica φ del espacio $\mathcal{U}$ en el espacio $\mathcal{V}$ que satisface las condiciones*

(1) $\varphi(\boldsymbol{e}_1) = c_1, \ldots, \varphi(\boldsymbol{e}_n) = \boldsymbol{c}_n$.

Demostración. Todo vector del espacio $\mathcal{U}$ puede ser representado bajo la forma de una combinación lineal de vectores de base, es decir bajo la forma de $\lambda_1 \boldsymbol{e}_1 + \ldots + \lambda_n \boldsymbol{e}_n$. Notece φ la funciòn de $\mathcal{U}$ en $\mathcal{V}$, definida por la igualdad

$$\varphi(\lambda_1 \boldsymbol{e}_1 + \ldots + \lambda_n \boldsymbol{e}_n) = \lambda_1 c_1 + \ldots + \lambda_n c_n$$

Para todos $\lambda_1, \ldots, \lambda_n$ de F.

Se constata sin problema que la función φ satisface a las condiciones (1)

La función φ satisface a las condiciones de linealida. En efecto, si $\mathbf{x} = \propto_1 \boldsymbol{e}_1 + \ldots + \propto_n \boldsymbol{e}_n$

Y $\boldsymbol{y} = \beta_1 \boldsymbol{e}_1 + \ldots + \beta_n \boldsymbol{e}_n$,

Entonces

$$\mathbf{x} + \mathbf{y} = (\propto_1 + \beta_1) e_1 + \ldots + (\propto_n + \beta_n) \boldsymbol{e}_n$$

$$\text{y } \lambda_x = \lambda_{\propto_1} e_1 + \ldots + \lambda_{\propto_n} x_n.$$

Por lo tanto, en virtud de la definición de la función φ,

$$\varphi(\mathrm{x}+\mathrm{y}) = (\propto_1 + \beta_1)c_1 + \ldots + (\propto_n + \beta_n)\mathrm{c}_n =$$
$$= (\propto_1 \mathrm{c}_1 + \ldots + \propto_n \mathrm{c}_n) + (\beta_1 \mathrm{c}_1 + \ldots + \beta_n \mathrm{c}_n) =$$
$$= \varphi(x) + \varphi(y);$$
$$\varphi(\lambda x) = \boldsymbol{\lambda}_{\propto_1} c_1 + \ldots + \boldsymbol{\lambda}_{\propto_n} c_n = \lambda(\propto_1 \mathrm{c}_1 + \ldots + \propto_n \mathrm{c}_n) =$$
$$= \lambda\varphi(\mathrm{x}).$$

Plantéese que ψ es una función lineal de $\mathcal{U}$ en $\mathcal{V}$ que satisface las condiciones $\psi(e_1) = \mathrm{c}_1, \ldots, \psi(e_n) = \mathrm{c}_n$. Entonces para todo vector $\mathrm{x} = \propto_1 \boldsymbol{e}_1 + \ldots + \propto_n \boldsymbol{e}_n$ del espacio $\mathcal{U}$, se cumple

$$\psi(x) = \propto_1 \psi(e_1) + \ldots + \propto_n \psi(e_n) = \propto_1 \mathrm{c}_1 + \ldots + \propto_n \mathrm{c}_n =$$
$$= \varphi(x),$$

Es decir $\psi = \varphi$.□

COROLARIO 1.2. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales sobre $\mathcal{F}$, $e_1, \ldots, e_n$ una base del espacio $\mathcal{U}$; φ y ψ funciones lineales de $\mathcal{U}$ en $\mathcal{V}$ tales que $\varphi(e_k) = \psi(e_k)$ para $k = 1, \ldots, n$ entonces $\varphi = \psi$.

COROLARIO 1.3. Sea $e_1, \ldots, e_n$ una base del espacio vectorial $\mathcal{V}$ y $\mathrm{c}_1, \ldots, \mathrm{c}_n$ vectores arbitrarios de este espacio. Entonces existe un operador lineal unico φ del espacio $\mathcal{V}$ que satisface a las condiciones (1).

Núcleo e imagen del operador lineal. Sea φ el operador lineal del espacio vectorial $\mathcal{V}$. El conjunto $\{x \in \mathrm{V} \mid \varphi(\mathrm{x}) = 0\}$se denota Ker φ. Dicho de otra manera, el conjunto Ker φ es una imagen inversa de vector nulo en la función φ,Ker $\varphi = \varphi^{-1}(0)$.En virtud de la linealidad del operador φ, este conjunto está cerrado respecto a la adición y a la multiplicación por escalares. Por lo tanto existe un subspacio del espacio $\mathcal{V}$ con conjunto de base Ker φ.

DEFINICIÓN. Un subespacio del espacio vectorial $\mathcal{V}$ con conjunto de base Ker φ es llamado núcleo del operador lineal φ y denotado $\mathcal{K}er\ \varphi$. La dimensión del núcleo lleva el nombre de defecto del operador φ, defecto $\varphi =$dim $\mathcal{K}er\ \varphi$.

El conjunto $\{\varphi(\mathrm{x}) \mid \mathrm{x} \in \mathrm{V}\}$se denota $\mathrm{Im}\ \varphi$ o $\varphi(V)$. En virtud de la linealidad del operador φ, este conjunto es cerrado respecto a la adición y multiplicación por escalares. Existe por tanto un subespacio del espacio $\mathcal{V}$con conjunto de base $\mathrm{Im}\ \varphi$.

DEFINICIÓN. Un subespacio del espacio vectorial $\mathcal{V}$ con conjunto de base $\mathrm{Im}\,\varphi$ es llamado imagen del operador lineal φ y se denota $\mathcal{Y}m\ \varphi$. La dimensión de la imagen del operador φ es llamado rango del operador φ, rango $\varphi = \dim(\mathcal{Y}m\ \varphi)$.

TEOREMA1.4. Sea φ un operador lineal de un espacio vectorial de dimensión finita $\mathcal{V}$. Entonces

(1) La suma del rango y del defecto del operador φ aplica $\dim \mathcal{V}$.

Demostración. Primer caso: Ker $\varphi = \{0\}$. Si $\mathcal{V} = \{0\}$, vemos inmediatamente que la conlusión del TEOREMA es verdadero.

supóngase que $\mathcal{V}$ es un espacio $\neq \{0\}$. Sean $\dim \mathcal{V} = n$ y $e_1, \ldots, e_n$ una base del espacio $\mathcal{V}$. Entonces, el sistema de vectores $\varphi(e_1), \ldots, \varphi(e_n)$ genera el espacio $\mathcal{Y}m\ \varphi$ es decir $\mathrm{Im}\varphi = L(\varphi(e_1), \ldots, \varphi(e_n))$.

Este sistema de vectores es linealmente independiente. En efecto si

$$\lambda_1\varphi(e_1) + \ldots + \lambda_n\varphi(e_n) = 0,$$

Entonces, en virtud de la linealidad del operador φ,

$$\varphi(\lambda_1 e_1 + \ldots + \lambda_n e_n) = 0$$

Como Ker $\varphi = \{0\}$ se deduce que

$\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$

Y en virtud de la independencia lineal de vectores, $\lambda_1 = 0, \ldots, \lambda_n = 0$. El sistema $\varphi(e_1), \ldots, \varphi(e_n)$ es así una base del espacio $\mathcal{Y}m\ \varphi$ y como resultado el rango φ equivale a n. Además, el defecto φ es igual a cero. Por lo tanto, la afirmación (1)se verifica.

Segundo caso: Ker $\varphi \neq \{0\}$. Planteese como defecto $\varphi = r$ y $e_1, \ldots, e_r$ es una base del núcleo del operador φ, la base del espacio $\mathcal{K}er\ \varphi$. Si $r = \dim \mathcal{V}$, entonces la afirmación (1)es aparantemente verdadera.

Admitase que $r < n = \dim \mathcal{V}$. En ese caso el sistema $e_1, \ldots, e_r$ puede ser completado hasta la base del espacio $\mathcal{V}$. Sea $e_1, \ldots, e_r, e_{r+1}, \ldots, e_n$la base del espacio $\mathcal{V}$; entonces

$\operatorname{Im} \varphi = L\big(\varphi(e_1), \ldots, \varphi(e_n)\big)$.

Dado que $\varphi(e_1) = 0, \ldots, \varphi(e_r) = 0$ tenemos

$\operatorname{Im} \varphi = L\big(\varphi(e_{r+1}), \ldots, \varphi(e_n)\big)$,

Dicho de otra manera, el sistema de vectores $\varphi(e_{r+1}), \ldots, \varphi(e_n)$ genera el espacio $\mathcal{Y}m\ \varphi$.

Este sistema es linealmente independiente. En efecto, si

$\lambda_{r+1}\ \varphi(e_{r+1}) + \ldots + \lambda_n \varphi(e_n) = 0$,

Entonces, en virtud de la linealidad del operador φ,

$$\varphi(\lambda_{r+1} e_{r+1} + \ldots + \lambda_n e_n) = 0,$$

De donde

$$\lambda_{r+1} e_{r+1} + \ldots + \lambda_n e_n \in \operatorname{K}er\varphi.$$

Ya que $e_1, \ldots, e_r$ es una base del espacio $\mathcal{K}er\ \varphi$, existen escalares $\lambda_1, \ldots, \lambda_r$ tales como

$$\lambda_{r+1} e_{r+1} + \ldots + \lambda_n e_n = \lambda_1 e_1 + \ldots + \lambda_r e_r$$

Y por lo tanto,

$$(-\lambda_1) e_1 + \ldots + (-\lambda_r) e_r + \lambda_{r+1} e_{r+1} + \ldots + \lambda_n e_n = 0.$$

En virtud de la independencia lineal de vectores$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ se deduce que todos los coeficientes del segundo miembro de la igualdad son nulos y en particular,$\lambda_{r+1} = 0, \ldots, \lambda_n = 0$. El sistema de vectores $\varphi(e_{r+1}), \ldots, \varphi(e_n)$es asi una base del espacio $\mathcal{Y}m\ \varphi$ y el rango φse aplica $n - r$. Por consiguiente la afirmación (1)es verdadera.□

Operaciones sobre funciones lineales. Sean $\mathcal{U}$ y $\mathcal{V}$ espacios vectoriales sobre la estructura $\mathcal{F}, \varphi, \psi$ de funciones lineales de $\mathcal{U}$ en $\mathcal{V}$. La suma $\varphi + \psi$ es definida como una función de $\mathcal{U}$ en $\mathcal{V}$ que asocia al elemento $\mathrm{x}\ \mathcal{U}$ del elemento $\varphi(\mathbf{x}) + \psi(\mathbf{x}) de\ \mathcal{V}$, es decir

$(\varphi + \psi)(\mathbf{x}) = \varphi(\mathbf{x}) + \psi(\mathbf{x})$.

El producto del escalar $\lambda \in F$ y de la función φ es definida como función de $\mathcal{U}$ en $\mathcal{V}$ que asocia al elemento $\mathrm{x} \in \mathcal{U}$ el elemento $\lambda\varphi(\mathrm{x})$del espacio $\mathcal{V}$, es decir $(\lambda\varphi)(\mathrm{x}) = \lambda\varphi(\mathrm{x})$.

PROPOSICIÓN 1.5. Sean φ y ψ funciones lineales del espacio vectorial $\mathcal{U}$ en el espacio vectorial $\mathcal{V}$ y $\lambda \in F$. Entonces $\varphi + \psi$ y $\lambda\varphi$ son funciones lineales de $\mathcal{U}$ en $\mathcal{V}$.

Demostración. La suma $\varphi + \psi$ satisface las condiciones de linealidad. En efecto, para todos $\mathbf{a}, \mathbf{b} \in \mathrm{U}$ y todo $\lambda \in F$, tenemos:

$(\varphi + \psi)(\mathrm{a} + \mathrm{b}) = \varphi(\mathrm{a} + \mathrm{b}) + \psi(\mathrm{a} + \mathrm{b}) = \varphi(\mathrm{a}) + \varphi(\mathrm{b}) +$

$+\psi(\mathrm{a}) + \psi(\mathrm{b}) = \varphi(\mathrm{a}) + \psi(\mathrm{a}) + \varphi(\mathrm{b}) + \psi(\mathrm{b}) =$

$$= (\varphi + \psi)(\mathrm{a}) + (\varphi + \psi)(\mathrm{b});$$

$$(\varphi + \psi)(\lambda \mathrm{a}) = \varphi(\lambda \mathrm{a}) + \psi(\lambda \mathrm{a}) = \lambda\varphi(\mathrm{a}) + \lambda\psi(\mathrm{a}) =$$

$$= \lambda(\varphi(\mathrm{a}) + (\mathrm{a})) = \lambda((\varphi + \psi)(\mathrm{a})).$$

Asi $\varphi + \psi$ es una función lineal de $\mathcal{U}$ en $\mathcal{V}$.

El producto $\lambda\varphi$ satisface las condiciones de linealidad. En efecto para todos $\mathbf{a}, \mathbf{b} \in \mathrm{U}$ y todo $\lambda \in F$ tenemos:

$$(\lambda\varphi)(\mathrm{a} + b) = \lambda\big(\varphi(\mathrm{a} + \mathrm{b})\big) = \lambda\big(\varphi(\mathrm{a}) + \varphi(\mathrm{b})\big) =$$

$$= \lambda\varphi(\mathrm{a}) + \lambda\varphi(\mathrm{b}) = (\lambda\varphi)(\mathrm{a}) + (\lambda\varphi)(b);$$

$$(\lambda\varphi)(\mu\mathrm{a}) = \lambda\varphi(\mu\mathrm{a}) = \lambda(\mu\varphi(\mathrm{a})) = (\lambda\mu)\varphi(\mathrm{a}) =$$

$$= \mu(\lambda\varphi(\mathrm{a})) = \mu\big((\lambda\varphi)(\mathrm{a})\big).$$

Por consiguiente, $\lambda\varphi$ es una función lineal de $\mathcal{U}$en $\mathcal{V}$.□

COROLARIO 1.6. El conjunto Hom $(\mathcal{U}, \mathcal{V})$es cerrado respecto a la adición y multiplicación por escalares.

Ejercicios

1. Sea φ un operador lineal del espacio vectorial unidimensional $\mathcal{V}$ sobre la estructura $\mathcal{F}$. Demostrar que existe un escalar $\lambda \in F$ tal que $\varphi(\mathrm{x}) = \lambda\mathrm{x}$ para todo vector $\mathbf{x} \in V$.
2. Sean φ y ψ operadores lineales del espacio vectorial de dimensión finita y $\varphi\psi = 0$. ¿Tendremos $\psi\varphi = 0$?
3. Sean φ una función lineal del espacio vectorial $\mathcal{U}$ en el espacio $\mathcal{V}$ y $\mathbf{b} \in \mathrm{Im}\,\varphi$. Demostrar que el conjunto $\varphi^{-1}(\mathbf{b})(\varphi^{-1}(\mathbf{b}) = \{\mathrm{x} \in V \mid \varphi(\mathrm{x}) = \mathbf{b}\})$ es una variedad lineal del espacio $\mathcal{U}$ de dirección $\mathcal{K}er\ \varphi$.
4. Sea φ una función lineal del espacio vectorial $\mathcal{U}$ en el espacio $\mathcal{V}$ y $\mathrm{a}_1, \ldots, \mathrm{a}_m \in U$. Demostrar que si el sistema $\varphi(\mathrm{a}_1), \ldots, \varphi(\mathrm{a}_m)$ es linealmente independiente en $\mathcal{V}$

El sistema $\mathrm{a}_1, \ldots, \mathrm{a}_m$ es entonces linealmente independiente en $\mathcal{U}$.

5. Sea φ una función lineal inyectiva del espacio vectorial $\mathcal{U}$ en el espacio $\mathcal{V}$. Demostrar que si el sistema $\mathrm{a}_1, \ldots, \mathrm{a}_m$ es linealmente independiente en $\mathcal{U}$, el sistema $\varphi(\mathrm{a}_1), \ldots, \varphi(\mathrm{a}_m)$ entonces es linealmente independiente en $\mathcal{V}$.
6. Demostrar que la función lineal φ del espacio vectorial $\mathcal{U}$ en el espacio $\mathcal{V}$ es inyectiva si y solo si $\mathcal{K}er\ \varphi = \{0\}$.
7. Sea φ una función lineal del espacio vectorial $\mathcal{U}$ en n dimensiones en el espacio $\mathcal{V}$ de dimensión n. Demostrar que φ es un isomorfismo.
8. Sea φ una función lineal del espacio vectorial $\mathcal{U}$ sobre esl espacio unidimensional $\mathcal{V}$ y a $\in U \setminus Ker\varphi$.Demostrar que $\mathcal{U} = \mathcal{K}er\ \varphi \oplus \mathcal{L}\,(\mathrm{a})$.
9. Sea φ, ψ operadores lineales del espacio vectorial $\mathcal{V}$ tales que $Ker\ \varphi = Ker\ \psi = \{0\}$. Demostrar que $Ker(\varphi\psi) = \{0\}$
10. Sea φ un operador lineal del espacio vectorial $\mathcal{V}$ que satisface a la condición $\varphi\ o\ \varphi = \varphi$.Mostrar que $\mathcal{V} = \mathcal{K}er\ \varphi \oplus \mathcal{Y}m\ \varphi$.
11. Sea $\mathcal{U}\ y\ \mathcal{V}$ espacios vectoriales sobre la estructura $\mathcal{F}$, el espacio $\mathcal{U}$ es unidimensional. Demostrar que toda función diferente de cero de $\mathcal{U}$ en $\mathcal{V}$ es inyectiva.
12. Sea $Hom\,(\mathcal{U}, \mathcal{V})$ un espacio vectorial de todas las funciones lineales del espacio vectorial $\mathcal{U}$ de dimensión finita en el espacio de dimensión finita $\mathcal{V}$. Demostrar que

(a) Si $\dim \mathcal{U} = 1$, entonces $\dim\big(Hom\,(\mathcal{U}, \mathcal{V})\big) = \dim \mathcal{V}$,

(b) Si $\dim \mathcal{V} = 1$, entonces $\dim\big(Hom\,(\mathcal{U}, \mathcal{V})\big) = \dim \mathcal{U}$.

13. Sea $\mathcal{U}\ y\ \mathcal{V}$ espacios vectoriales de dimensión finita cuyas dimensiones son m y n. Demostrar que la dimensión del espacio vectorial $Hom\ (\mathcal{U},\mathcal{V})$ equivale al producto mn.

14. Sea φ la función lineal del espacio vectorial de dimensión finita $\mathcal{U}$ en el espacio vectorial $\mathcal{V}$. Demostar que $\dim(\mathcal{K}er\ \varphi)+\dim(\mathcal{Y}m\ \varphi)=\dim\mathcal{U}$.

15. Sea φ una función lineal del espacio vectorial $\mathcal{U}$ en el espacio vectorial de dimensión finita $\mathcal{V}$. Sea $\mathrm{a}_1,\ .\ .\ .\ ,\mathrm{a}_m$ un sistema de vectores del espacio $\mathcal{U}$ tal que el sistema $\varphi(\mathrm{a}_1),\ .\ .\ .\ ,\varphi(\mathrm{a}_m)$ sea una base del espacio $\mathcal{Y}m\ \varphi$. Demostrar que $\mathcal{U}=\mathcal{K}er\ \varphi\oplus\mathcal{L}(\mathrm{a}_1,\ .\ .\ .\ ,\mathrm{a}_m)$.

16. Sea φ un operador lineal del espacio vectorial de dimensión finita $\mathcal{V}$ en el cuerpo $\mathcal{F}$. Demostrar que para un número natural suficientemente grande m los operadores lineales $\varphi,\varphi^2,\ldots,\varphi^m$ son lineamente dependientes en el cuerpo $\mathcal{F}$.

§ 2. Representación de operadores lineales por matrices.

Matriz de un operador lineal: Sea $\mathcal{V}$ un espacio vectorial de dimensión finita en el cuerpo$\mathcal{F}$,

(1) $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_n$

siendo su base y φ el operador lineal del espacio $\mathcal{V}$. Represéntese los vectores $\varphi(\boldsymbol{e}_1),\ldots,\varphi(\boldsymbol{e}_n)$ bajo forma de combinación lineales de vectores de la base (1):

$$\begin{aligned}&\varphi(\boldsymbol{e}_1)=a_{11}\boldsymbol{e}_1+\ldots+a_{n1}\boldsymbol{e}_n,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\varphi(e_n)=a_{1n}\boldsymbol{e_1}+\boldsymbol{\ldots}+a_{nn}\boldsymbol{e}_n.\end{aligned}\qquad(2)$$

DEFINICIÓN: La matriz $\mathrm{M}(\varphi)$

$$M(\varphi)=\begin{bmatrix}a_{11}\ldots a_{1n}\\ \ldots\ldots\ldots\\ a_{1n}\ldots a_{nn}\end{bmatrix}$$

Cuya $\mathcal{K}$- ésima columna es la columna de coordenadas de vectores $\varphi(e_k)$ relativamente en la base (1), se llama $matriz\ del\ operador\ lineal\ \varphi\ relativamente\ en\ la\ base\ (1)$

Recordemos que $\mathrm{F}^{n\times n}$ designa el conjunto de todas las matrices $n\times n$ en el cuerpo $\mathcal{F}$.

TEOREMA 2.1. Sea $\mathcal{V}$ un espacio vectorial en el cuerpo $\mathcal{F}$ con una base (1) fija. La función Φ que asocia cada operador lineal φ del espacio $\mathcal{V}$ su matriz $\mathcal{M}(\varphi)$ relativamente en la base (1), es una función biyectiva del conjunto $\mathrm{H}om(\mathcal{V},\mathcal{V})$ en el conjunto F^{nxn}. Demostración. Φ Es aparentemente una función en el conjunto F^{nxn}. Demuéstrese que la función Φes inyectiva, es decir que para todos φ y ψ de la igualdad $M(\varphi)=M(\psi)$ seguido de la igualdad $\varphi=\psi$. De $M(\varphi)=M(\psi)$ se obtiene la igualdad

$M(\varphi(\boldsymbol{e}_k))=M(\psi(\boldsymbol{e}_k))$ Para $k=1,\ldots,n$,

De donde

$\varphi(e_k)=\psi(e_k)$ Para $\mathcal{K}=1,\ldots,n$.

Según el corolario 1.2se deduce la igualdad $\varphi=\psi$. ■

Sea λ un escalar, $\lambda\in\mathrm{F}$. notemos $\omega_\lambda$la operación singular (unaria) en el conjunto $\mathrm{H}om(\mathcal{U},\mathcal{V})$ que asocia cada función lineal $\varphi\in\mathrm{H}om(\mathcal{U},\mathcal{V})$ la función lineal $\lambda\varphi$: $\omega_\lambda=\lambda_\varphi$

Esta operación será llamada *operación de multiplicación por el escalar* λ.

TEOREMA 2.2 sean $\mathcal{U},\mathcal{V}$ *los espacios vectoriales en el cuerpo*$\mathcal{F}$.

El álgebra

Según el corolario 1.2se deduce la igualdad $\varphi = \psi$. ■

Sea λ un escalar, $\lambda \in \mathrm{F}$. notemos $\omega_\lambda$la operación singular (unaria) en el conjunto $\mathrm{H}om(\mathcal{U}, \mathcal{V})$ que asocia cada función lineal $\varphi \in \mathrm{H}om(\mathcal{U}, \mathcal{V})$ la función lineal $\lambda\varphi$: $\omega_\lambda = \lambda_\varphi$

Esta operación será llamada *operación de multiplicación por el escalar* λ.

TEOREMA 2.2 sean $\mathcal{U}, \mathcal{V}$ *los espacios vectoriales en el cuerpo* $\mathcal{F}$.

El álgebra

$$\langle \mathcal{H}om(\mathcal{U}, \mathcal{V}), +, -, \{\omega_{\lambda|}\, \lambda \in \mathrm{F}\}\rangle$$

Es un espacio vectorial en el cuerpo $\mathcal{F}$.

Demostración. Según el corolario 1.2 el conjunto $\mathrm{H}om(\mathcal{U}, \mathcal{V})$ es cerrado en relación a la adición y en las operaciones singulares (unarias) ω_φ de multiplicación por los corolarios del cuerpo$\mathcal{F}$.

Nótese que " – " designa una operación lineal singular (unaria) en el conjunto $\mathrm{H}om(\mathcal{U}, \mathcal{V})$ que asocia al operador $\varphi \in \mathrm{H}om(\mathcal{U}, \mathcal{V})$ el operador $-\varphi = (-1)\varphi$, y 0 la función cero de $\mathcal{U}$ en $\mathcal{V}$.

El algebra $\langle \mathrm{H}om(\mathcal{U}, \mathcal{V}), +, -\rangle$ es un grupo abeliano. De hecho se verifica sin duda alguna que para todos $\varphi, \psi, \chi \in \mathrm{H}om(\mathcal{U}, \mathcal{V})$ se tiene las igualdades

$\varphi + \psi = \psi + \varphi$. $\varphi + \bar{0} = \varphi$,

$\varphi + (\psi + \chi) = (\varphi + \psi) + \chi$, $\varphi + (-\varphi) = \bar{0}$.

Por otra parte, se verifica fácilmente que para todos $\varphi, u \in \mathrm{F}$ se tiene

$\lambda(\varphi + \psi) = \varphi_\psi + \varphi_{\psi,}$ $(\varphi_u)\lambda(u\varphi)$,

$(\lambda + u)\,\lambda_\varphi + u_{\varphi,}$ $1.\ \varphi = \varphi$.

Entonces, todos los axiomas del espacio vectorial se verifican. ■

El espacio vectorial

$$\langle \mathrm{H}om(\mathcal{U}, \mathcal{V}), +, -, \{\omega'_\lambda \mid \lambda \in \mathrm{F}\}\rangle$$

Será llamado *espacio vectorial de las funciones lineales* $\mathcal{U}$ *en* $\mathcal{V}$ se denotará

$\mathcal{H}om(\mathcal{U}, \mathcal{V})$.

Conexión entre las columnas de coordenadas de vectores $\mathbf{x}$ y $\boldsymbol{\varphi}(\mathbf{x})$. Siendo

(1) $e_1, \ldots, e_n$

la base fija del espacio vectorial $\mathcal{V}$ y φ el operador lineal de este espacio. Siendo, entonces

$\mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n$ Y $\varphi(\mathbf{x}) = \eta_1\mathbf{e}_1 + \ldots + \eta_\eta\ \mathbf{e}_{n.}$

Nótese $M(\mathbf{x})$y $M(\varphi(\mathbf{x}))$ las columnas de coordenadas respectivamente de los vectores $\mathbf{x}$ y $\varphi(\mathbf{x})$ relativamente en la base fija (1):

$$M(\mathbf{x})\begin{bmatrix}\xi_1\\ \cdot\\ \cdot\\ \cdot\\ \xi_n\end{bmatrix}, \qquad M\big(\varphi(\mathbf{x})\big) = \begin{bmatrix}n_1\\ \cdot\\ \cdot\\ \cdot\\ n_n\end{bmatrix}.$$

Búsquese la conexión entre estas columnas de coordenadas.

TEOREMA 2.3. Sea φ el operador lineal del espacio vectorial $\mathcal{V}$ y $M(\varphi)$ la matriz del operador φ relativamente en la base (1).

Entonces para todo vector $\mathbf{x} \in \mathcal{V}$ se satisface la igualdad

$M\big(\varphi(\mathbf{x})\big) = M(\varphi)\,M(\mathbf{x})$.

Demostración. Sea

$$M(\varphi) = \begin{bmatrix} a_{11} \ldots a_{1n} \\ \ldots\ldots \\ a_{n1} \ldots a_{nn} \end{bmatrix},$$

Las igualdades (2) son entonces verificadas. Si $\mathbf{x} = \xi_1 e_1 + \ldots + \xi_n e_n \in \mathcal{V}$, entonces $\varphi(\mathbf{x}) = \xi_1 \varphi(e_1) + \ldots + \xi_n \varphi(e_n)$.

Al sustituir la base (2) en esta igualdad de vectores $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$, se obtiene

$\varphi(\mathbf{x}) = \xi_1(a_{11}\boldsymbol{e}_1 + \ldots + a_{n1}\boldsymbol{e}_n) + \ldots + \xi_n(a_{1n}\boldsymbol{e}_1 + \ldots\ldots + a_{nn}\boldsymbol{e}_n)$,

de donde

$\varphi(\mathbf{x}) = (a_{11}\xi_1 + \ldots + a_{1n}\xi_n)\boldsymbol{e}_1 + \ldots + (a_{n1}\xi_1 + \ldots\ldots + a_{nn}\xi_n)\boldsymbol{e}_n$.

Por tanto,

$$M(\varphi(\mathbf{x})) = \begin{bmatrix} a_{11}\xi_1 + \ldots + a_{1n}\xi_n \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}\xi_1 + \ldots + a_{nn}\xi_n \end{bmatrix} = \begin{bmatrix} a_{11} \ldots a_{1n} \\ \ldots\ldots\ldots \\ a_{n1} \ldots a_{nn} \end{bmatrix} \cdot \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix},$$

Es decir $M(\varphi(\mathbf{x})) = M(\varphi)M(\mathbf{x})$. ■

TEOREMA 2.4. Siendo φ el operador lineal del espacio vectorial $\mathcal{V}$ y $M(\varphi)$ la matriz del operador φ relativamente en la base fija (1).

Si para cualquier vector $\mathbf{x} \in V$ se tiene

(1) $M(\varphi(\mathbf{x})) = \mathrm{B}M(\mathbf{x})$,

Entonces $\mathrm{B} = M(\varphi)$.

Demostración. Según la definición de la matriz $\mathrm{M}(\varphi)$,

(2) $M(\varphi) = \left(M(\varphi(e_1)), M(\varphi(e_2)), \ldots, M(\varphi(e_n))\right)$.

Incorporando sucesivamente en (3) en lugar de **x** los vectores de base $\mathbf{e}_1, \ldots, \mathbf{e}_n$, se obtiene

$$M(\varphi(\mathbf{e}_1)) = \mathrm{B}M(\mathbf{e}_1) = \mathrm{B}\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \mathrm{B}^1;$$

$$(3)\quad M(\varphi(\mathbf{e}_2)) = \mathrm{B}M(\mathbf{e}_2) = \mathrm{B}\begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \mathrm{B}^2$$

. . . . . .

$$M(\varphi(\mathbf{e}_n)) = \mathrm{B}M(\mathbf{e}_n) = \mathrm{B}\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \mathrm{B}^n.$$

En la base de (4) y (5) se concluye que las columnas correspondientes a las matrices $M(\varphi)$ y B coinciden. Por tanto, $M(\varphi) = \mathrm{B}$. ■

PROPOSICION 2.5. Siendo φ y ψ los vectores lineales del espacio vectorial $\mathcal{V}$ en la base fija $\mathbf{e}_1, \ldots, \mathbf{e}_n$ y $\lambda \in \mathcal{F}$; entonces

(1) $M(\varphi + \psi) = M(\varphi) + M(\psi)$;

(2) $M(\lambda_\varphi) = \lambda M(\varphi)$

Demostración. Sea $\mathbf{x} \in \mathrm{V}$ y

$$\varphi(\mathbf{x}) = \xi_1 \mathbf{e_1} + \ldots + \xi_n \mathbf{e}_n;$$

(3)

$$\psi(x) = \eta_1 \mathbf{e}_1 + \cdots + \eta_n \mathbf{e}_n,$$

Entonces

$$(\varphi + \psi)(x) = (\xi_1 + \eta_1)\mathbf{e}_1 + \ldots + (\xi_n + \eta_n)\mathbf{e}_n$$

Por tanto,

$$M\big((\varphi + \psi)(x)\big) = \begin{bmatrix} \xi_1 + \eta_1 \\ \ldots\ldots \\ \xi_n \quad \eta_n \end{bmatrix} = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} + \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix} = M\big(\varphi(\mathbf{x})\big) + M(\psi(\mathbf{x}))$$

Y, según el TEOREMA 2.3,

(4) $M\big((\varphi + \psi)(\mathbf{x})\big) = (M(\varphi) + M(\psi))M(\mathbf{x})$

La igualdad (4) es verdadera para todo $x \in V$. Según el TEOREMA 2.4 de (4) se deduce la igualdad (1)

En virtud de (3). $\big(\lambda_\varphi\big)(\mathbf{x}) = \lambda\, \xi_1 \mathbf{e}_1 + \ldots \lambda \xi_n \mathbf{e}_{n;}$ Por tanto,

$$M\left(\big(\lambda_\varphi\big)(\mathbf{x})\right) = \lambda M(\varphi(\mathbf{x}))$$

Y según el TEOREMA 2.3, para todo **x** se tiene

(5) $M\big((\lambda\varphi)(\mathbf{x})\big) = \big(\lambda M(\varphi)\big)M(\mathbf{x})$.

Según el TEOREMA 2.4 de (5) se deduce (2). ■

Rango de un operador lineal. Establézcase la conexión entre el rango de un operador lineal y el rango de su matriz.

TEOREMA 2.6. *El rango de un operador lineal de un espacio vectorial de dimensión finita* $\neq \{0\}$*es igual al rango de la matriz de este operador.*

Demostración. Sea $\mathbf{e_1}, \ldots, \mathbf{e}_n$ la base fija del espacio vectorial $\mathcal{V}$. Siendo $M\big(\varphi(\mathbf{e}_1)\big), \ldots, M(\varphi(\mathbf{e}_n))$ las columnas de las coordenadas de los vectores

$\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ relativamente en la base fija. Estas son columnas de la matriz $M(\varphi)$ del operador φ relativamente en la base fija, es decir

$M(\varphi) = (M\big(\varphi(\mathbf{e}_1)\big), \ldots, M(\varphi(\mathbf{e}_n)))$

Por tanto,

(1) Rango $M(\varphi) =$ rango$\big(M(\varphi(\mathbf{e}_1)\big), \ldots, M(\varphi(\mathbf{e}_n)))$.

En virtud del corolario 7.3, el rango del sistema de vectores $\varphi(\boldsymbol{e}_1), \ldots\ldots, \varphi(\mathbf{e}_n)$ es igual al rango del sistema de columnas de estos vectores.

De ahí y a partir de (1) se deduce que

(2) rango $M(\varphi) =$rango$(\varphi(\mathbf{e}_1), \ldots . \varphi(\mathbf{e}_n))$.

Siendo $\mathbf{x}$ un vector arbitrario del espacio $\mathcal{V}$y $\mathbf{x} = \xi_1 \boldsymbol{e}_1 + \ldots\ldots + \xi_1 \boldsymbol{e}_n$. En virtud de la linealidad del operador φla igualdad $\varphi(\mathbf{x}) = \xi_1 \varphi(\mathbf{e}_1) + \ldots + \xi_n \varphi(\mathbf{e}_n)$ se verifica.

Así pues tenemos

$\mathrm{Im}(\varphi) = \mathrm{L}(\varphi(\mathbf{e}_1), \ldots, \varphi\,(\mathbf{e}_n))$,

Es decir que los vectores $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ generan la imagen del operador φ Según el corolario 7.3, se deduce que

(3) rango $\varphi =$ rango $\big(\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)\big)$.

En la base de (2) y (3) se concluye que el rango φ es igual al rango de la matriz $M(\varphi)$. □

Conexión entre las columnas de las coordenadas de un vector relativamente en diferentes bases. Sea $\mathcal{V}$ un espacio vectorial de dimensión $n \neq \{0\}$ en el cuerpo $\mathcal{F}$. Dadas dos bases de este espacio: $\mathbf{e}_1, \ldots, \mathbf{e}_n$, la primera base y $\mathbf{e}'_1, \ldots, \mathbf{e}'_n$, la segunda. Los vectores de la segunda base serán representados en forma de combinaciones lineales de la primera base:

$\mathbf{e}'_1 = t_{11}\mathbf{e}_1 + \ldots + t_{n1}\mathbf{e}_n$

(1). . . . . $(t_{ik} \in F)$

$\mathbf{e}'_1 = t_{1n}\mathbf{e}_1 + \ldots + t_{nn}\mathbf{e}_n$

Se llama matriz de transición de la primera base a la segunda la matriz T ,

$$T = \begin{bmatrix} t_{11}t_{12}\ldots t_{in} \\ t_{21}t_{22}\ldots t_{2n} \\ \ldots\ldots\ldots \\ t_{n1}t_{n2}\ldots t_{nn} \end{bmatrix},$$

Por tanto la *k*- ésima columna es la columna de coordenadas de vectores $\mathbf{e}'_k$relativamente en la primera base.

PROPOSICION 2.7. *La matriz T es inversible*

Demostración. Se deduce de la independencia lineal de los vectores: $\mathbf{e}'_1, \ldots, \mathbf{e}'_n$, la independencia lineal de las columnas de coordenadas de estos vectores, es decir, la independencia lineal de columnas de la matriz T (ver corolario 7.4). Se deduce, según el TEOREMA 5.1, que la matriz T es inversible □

Nótese $M(\mathbf{x})$ la columna de coordenadas de los vectores $\mathbf{x} \in \mathcal{V}$ relativamente en la primera base y $M'(\mathbf{x})$ relativamente en la segunda base. Búsquese la relación entre $M(\mathbf{x})$ y $M'(\mathbf{x})$

TEOREMA 2.8. Siendo $M(\mathbf{x})$ y $M'(\mathbf{x})$ *las columnas de coordenadas de los vectores $\boldsymbol{x}$ respectivamente relativo a la primera y a la segunda base y T la matriz de transición de la primera base del espacio en la segunda. Entonces tenemos las igualdades*

(2) $M(\mathbf{x}) = TM'(\mathbf{x})$

(3) $M'(\mathbf{x}) = T^{-1}M(\mathbf{x})$

Demostración. sea $\mathbf{x} \in V$ y

(4) $\mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\boldsymbol{e}_n$;

(5) $\mathbf{x} = \xi'_1\mathbf{e}'_1 + \ldots + \xi'_n\boldsymbol{e}'_n$

Por consiguiente,

$$M(\boldsymbol{x})\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \qquad M'(\boldsymbol{x})\begin{bmatrix} \xi'_1 \\ \vdots \\ \xi'_n \end{bmatrix},$$

Llevemos en (5) las expresiones de $\mathbf{e}'_1, \ldots, \mathbf{e}'_n$ las igualdades (1), encontramos

$$x = \xi'_1(t_{11}e_1 + \ldots + t_{n1}\boldsymbol{e}_n) + \ldots + \xi'_1(t_{1n}e_1 + \ldots\ldots + t_{nn}\boldsymbol{e}_n,)$$

De donde

(6) $x = (t_{11}\xi'_1 + \ldots + t_{1n}\xi'_n)\mathbf{e}_1 + \ldots\ldots + (t_{n1}\,\xi'_n + \ldots + t_{nn}\xi'_n)\boldsymbol{e}_n$

A partir de (4) y (6) se deducen las igualdades

$\xi_1 = t_{11}\xi'_1 + \ldots + t_{1n}\xi'_n$;

. . . . . .

$\xi_n = t_{n1}\xi'_1 + \ldots + t_{nn}\xi'_n$

De esto se obtiene la igualdad

$$\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix} = T\begin{bmatrix}\xi'_1\\ \vdots\\ \xi'_n\end{bmatrix}$$

Es decir que $M(\mathbf{x}) = TM'(\mathbf{x})$

Multiplíquese a la izquierda los dos elementos de esta igualdad por T^{-1} y se obtiene (3) ■

COROLARIO 2.9. Si ${}^{t}M(\mathbf{x})$ y ${}^{t}M'(\mathbf{x})$ *son líneas de coordenadas del vector* $\mathbf{x}$ *respectivamente en relación a la primera y a la segunda base, obtenemos entonces*

${}^{t}M(\mathbf{x}) = {}^{t}M'(\mathbf{x})^{t}T$, ${}^{t}M(\mathbf{x}) = {}^{t}M(\mathbf{x})^{t}(T^{-1})$.

Conexión entre las matrices de un operador lineal relativamente en diferentes bases. Sea $\mathcal{V}$ un espacio vectorial de dimensión finita $\neq \{0\}, \mathbf{e}_1, \ldots, \mathbf{e}_n$ la primera base del espacio $\mathcal{V}$, $\mathbf{e}'_1, \ldots, \mathbf{e}'_n$ la segunda base del espacio $\mathcal{V}$ y T la matriz de transición de la primera en la segunda base.

TEOREMA 2.10. *Sea* φ *el operador lineal del espacio vectorial* $\mathcal{V}$, $M(\varphi)$ *y* $M'(\varphi)$ *las matrices de este operador respectivamente en relación a la primera y a la segunda base y* T *la matriz de transición de la primera en la segunda base, tenemos entonces* $M'(\varphi) = T^{-1}M(\varphi)T$.

Para todo Demostración. Según el TEOREMA $x \in V$,

Se tiene

(2) $M(\mathbf{x}) = TM'(\mathbf{x})$;

(3)$M'(\mathbf{x}) = T^{-1}M(\mathbf{x})$,

Donde $M(\mathbf{x})$y $M'(\mathbf{x})$ son columnas de coordenadas del vector $\mathbf{x}$ respectivamente por transición en la primera y en la segunda base. Sustituyéndose en (3) $\varphi(x)$ en $\mathbf{x}$, se tiene

$M'\big(\varphi(\mathbf{x})\big) = T^{-1}M\big(\varphi(\mathbf{x})\big)$.

Según el TEOREMA 2.3, $M\big(\varphi(\mathbf{x})\big) = M(\varphi)M(\mathbf{x})$, por tanto,

$M'\big(\varphi(\mathbf{x})\big) = T^{-1}M(\varphi)M(\mathbf{x})$.

En virtud (2), se tiene

$M'\big(\varphi(x)\big) = [T^{-1}M(\varphi)T]M'(\mathbf{x})$.

Dado que esta igualdad se verifica para todo $\mathbf{x}$ de V, se tiene en virtud del TEOREMA 2.4,$M'(\varphi) = T^{-1}M(\varphi)T$■.

DEFINICIÓN: L a matriz A y B del conjunto F^{n*n} se denominan *semejantes en el cuerpo* $\mathcal{F}$ si existe una matriz inversible $T \in F^{n*n}$ tal que $A = T^{-1}BT$.

Del TEOREMA 2.10 resulta el corolario siguiente.

COROLARIO 2.11. *Si* φ*es un operador lineal del espacio vectorial* $\mathcal{V}$ *de dimensión finita no reducida en* $\{0\}$*, entonces las matrices de este operador reportadas en dos bases cuales quiera del espacio son semejantes.*

PROPOSICION 2.12. *La relación de la similitud de matrices en el conjunto* F^{n*n} *es una relación de equivalencia.*

Demostración. la relación de similitud es reflexiva, ya que $A = E^{-1}AE$, donde E es una matriz unida. La relación de similitud es simétrica, puesto que la igualdad $A = T^{-1}BT$ se deduce $B(T^{-1})^{-1}AT^{-1}$. La relación de similitud es transitiva, ya que $A = T^{-1}BT$ y $B = T_1^{-1}CT_1$se deduce

$A = (T_1T)^{-1}C(T_1T)$.

La relación de similitud de matrices en el cuerpo $\mathcal{F}$ define la división del conjunto F^{n*n}en clases de equivalencia llamadas *clases de matrices semejantes.* A cada operador lineal del espacio vectorial $\mathcal{V}$ es asociada una clase única de matrices semejantes.

Ejercicios.

1. ¿Cómo variará la matriz de un operador lineal si cambiase en la base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ dos cuales quieras los vectores, por ejemplo, $\mathbf{e}_1$ y $\mathbf{e}_2$?
2. Demostrar que el rango del operador lineal de un espacio vectorial de dimensión finita es igual al rango de la matriz de este operador.
3. Mostar que todo operador lineal del rango r de un espacio vectorial de dimensión finita puede ser representado en forma de una suma de r operadores lineales del rango 1.
4. Sea $\mathcal{V}$un espacio vectorial de todas las matrices cuadradas de orden dos en el cuerpo$\mathcal{F}$. Mostrar que la transformación φ consiste en la multiplicación de matrices de $\mathcal{V}$a la izquierda por matriz $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$es un operador lineal. Buscar la matriz del operador φen la base

   $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$.
5. Demostrar que el operador lineal φ del espacio vectorial de dimensión finita $\mathcal{V}$, permutable con cada operador lineal del espacio $\mathcal{V}$,es un escalar, es decir que existe un escalar λ tal que $\varphi(\mathbf{x}) = \lambda\mathbf{x}$ para todo vector $\mathbf{x}$ de $\mathcal{V}$.
6. Sea φ un operador lineal cuales quiera, ψ un operador lineal inversible del espacio vectorial de dimensión finita. Demostrar que el rango $(\varphi\psi)$ =rango$(\psi\varphi)$ = rango φ.
7. Sea φ, ψ los operadores lineales cuales quiera de un espacio vectorial de dimensión finita. Demostrar que:

(a) rango $(\varphi + \psi) \leq$ rango φ +rango ψ;
(b) rango $(\varphi\psi) \leq$ rango φ, rango $(\varphi\psi) \leq$ rango ψ;
(c) def $\varphi \leq$ def$(\varphi\psi) \leq$ def φ +def ψ.

8. Dar un ejemplo del operador lineal φ, ψ de un espacio vectorial bidimensional para el cual rango $(\varphi, \psi) \neq$ rango $(\varphi\psi)$.
9. Demostrar que para todos los operadores lineales φ, ψ de un espacio vectorial de dimensión n satisface la igualdad
   rango $(\varphi\psi) \geq$ rango φ +rango $\psi - n -$.
10. Sea φ un operador lineal del espacio vectorial $\mathcal{V}$. El espacio interno $\mathcal{L}$ del espacio $\mathcal{V}$ es llamado *invariante relativamente* en φ si $\varphi(L) \subset L$. Supóngase que el operador φ posee relativamente en la base $e_1, \ldots, e_n$ una matriz diagonal en elementos diagonales diferentes. Búsquese todos los espacios internos $\mathcal{V}$ invariantes relativamente en φ y muéstrese que vale 2^n.

§ 3. Algebras Lineales.

Algebra lineal: Sea $\mathcal{F}$ un cuerpo de escalares.

DEFINICIÓN: El algebra $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}, . \rangle$ Es llamada *algebra lineal* si las operaciones binarias $+$, . y las operaciones singulares ω_λ satisfacen a las exigencias siguientes:

1) El algebra $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$ es un espacio vectorial en el cuerpo $\mathcal{F}$;

2) Las condiciones de bilinealidad se cvumplen, es decir

$(\mathbf{a} + \mathbf{b})c = \mathbf{ac} + \mathbf{bc}$, $\quad \mathbf{c}\,(\,\mathbf{a} + \boldsymbol{b}) = \boldsymbol{c}\mathbf{a} + \boldsymbol{cb}$

$\omega_\lambda(\mathbf{a}\boldsymbol{b}) = (\omega_\lambda\mathbf{a})\boldsymbol{b} = \boldsymbol{a}(\omega_\lambda\boldsymbol{b})$

Para todos $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$ y todo $\lambda \in F$. Llámese *rango del algebra lineal* a la dimensión del espacio vectorial $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$.

Ejemplos:

1. Sea $\mathbf{C}$ el conjunto de todos los números complejos. El algebra.

$\langle C, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, . \rangle$

Es una algebra lineal del cuerpo $\mathcal{R}$ de números reales. Su rango vale dos.

2. Sea F^{n*n} un conjunto de todas las matrices $n \times n$ sobre un cuerpo. El algebra

$\langle F^{n*n}, +, \{\omega_\lambda \mid \lambda \in F\}, . \rangle$,

Donde $\omega_\lambda$es una operación singular (unaria) de multiplicación por el escalar λ, constituye un algebra lineal en el cuerpo $\mathcal{F}$ del rango n^2. Se llama *algebra matricial completa en el cuerpo* $\mathcal{F}$. Su rango vale n^2.

3. El álgebra de Cuaternion en el cuerpo $\mathcal{R}$ siendo fija, sea V un espacio vectorial de dimensión cuatro en el cuerpo $\mathcal{R}$ y $\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ su base.

Defínase la multiplicación de vectores de base por las igualdades siguientes:

$$\mathbf{i^2} = \mathbf{j^2} = \mathbf{k^2} = -\mathbf{e}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \mathbf{ki} = -\mathbf{ik} = \mathbf{j};$$

$\mathbf{ae} = \mathbf{ea}$ Para todo vector $\mathbf{a} \in \{\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$.

El producto de dos Cuaternion cuales quiera es definido por la igualdad

$(a\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})(a_1\mathbf{e} + \beta_1\mathbf{i} + \gamma_1\mathbf{j} + \delta_1\mathbf{k}) = (aa_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\mathbf{e} + (a\beta_1 + \beta a_1 + \gamma\delta_1 - \delta\gamma_1)\mathbf{i} +$
$(a\gamma_1 + a_1\gamma + \delta\beta_1 - \beta\delta_1)\mathbf{j} + (a\delta_1 + a_1\delta + \beta\gamma_1 - \gamma\beta_1)\mathbf{k}$.

Los cuaterniones $\mathbf{q} = a\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ y $\overline{q} = a\mathbf{e} - \beta\mathbf{i} - \gamma\mathbf{j} - \delta\mathrm{k}$ se llaman conjugados. El valor real

$N(q) = q.\overline{q} = a^2 + \beta^2 + \gamma^2 + \delta^2$

Se llama *norma del Cuaternion.*

Una verificación directa muestra que las condiciones de bilinearidad están satisfechas. El algebra

$\langle V, +, \{\omega_2 \mid \lambda \in \mathbf{R}\}, . \rangle$

Es entonces lineal. Se llama *álgebra de Cuaternion* en los cuerpos de valores reales. Se verifica fácilmente que el álgebra $\langle V, +, -, ., \mathbf{e}\rangle$ es un aro no conmutativo, en el cual para todos $\boldsymbol{a}, \mathbf{b} \in V$ con $\mathbf{a} \neq 0$ la ecuación $\mathbf{ax} = \mathbf{b}$ se resuelve.

Algebra de operadores lineales de un espacio vectorial. Sea $\mathcal{V}$ un espacio vectorial en el cuerpo $\mathcal{F}$ y φ, ψ los operadores lineales de este espacio. El producto φ, ψ es definido como producto de φ y ψ, es decir como la función del espacio $\mathcal{V}$ en el mismo asociado en el elemento $\mathbf{x}$ de V el elemento $\varphi\big(\psi(\mathbf{x})\big)$:

$(\varphi\psi)(\mathbf{x}) = \varphi\big(\psi(\mathbf{x})\big)$.

PROPOSICION 3.1. Un *producto de dos cuales quiera operadores lineales del espacio vectorial* $\mathcal{V}$ es un operador lineal de este espac*io.*

Demostración. sea φ y ψ, los operadores lineales del espacio $\mathcal{V}$. El producto $\varphi\psi$satisface las condiciones de linealidad.

De hecho, si $\mathbf{x}, \mathbf{y} \in V$ y $\lambda \in F$, entonces

$$(\varphi\varphi)(\mathbf{x}+\mathbf{y}) = \varphi\big(\psi(\mathbf{x}+\mathbf{y})\big) = \varphi\big(\psi(\mathbf{x})+\psi(\mathbf{y})\big) = \varphi\big(\psi(\mathbf{x})\big)+\varphi\big(\psi(\mathbf{y})\big) = (\varphi\psi)(\mathbf{x})+(\phi\psi)(\mathbf{y}); (\varphi\psi)(\lambda\mathbf{x}) = \varphi\big(\psi(\lambda\mathbf{x})\big) = \varphi\big(\lambda\psi(\mathbf{x})\big) = \lambda(\varphi(\psi))) = \lambda((\varphi\psi)(\mathbf{x})).$$

Al igual, el producto $\varphi\psi$ es un operador lineal del espacio $\mathcal{V}$. ■

Sea $\mathcal{V}$ un espacio vectorial en el cuerpo $\mathcal{F}$. En virtud del corolario 1.6, $\mathcal{H}om(\mathcal{V},\mathcal{V})$ es un espacio vectorial en el cuerpo$\mathcal{F}$:

$\mathcal{H}om(\mathcal{V},\mathcal{V}) = \langle \mathrm{Hom}(\mathcal{V},\mathcal{V}), +\{\omega'_\lambda \mid \lambda \in \mathrm{F}\}\rangle,$

Donde ω'_λ es una operación singular (unaria) de multiplicación de operadores lineales del espacio $\mathcal{V}$ por el escalar λ. Considérese el álgebra

$\langle Hom(\mathcal{V},\mathcal{V}), +, \{\omega'_\lambda \mid \lambda \in \mathrm{F}\}, . \rangle,$

Donde la operación vinaria "." Es una operación de multiplicación de operadores lineales del espacio $\mathcal{V}$; esta algebra se llama á*lgebra de operadores lineales del espacio* $\mathcal{V}$ *y se denota End* $\mathcal{V}$.

TEOREMA 3.2. Sea $\mathcal{V}$ *un espacio vectorial en el cuerpo*$\mathcal{F}$. *El álgebra End* $\mathcal{V}$ *es un álgebra lineal en el cuerpo*$\mathcal{F}$.

Demostración. según el TEOREMA 2.2, el álgebra

$\langle Hom(\mathcal{V},\mathcal{V}), +, \{\omega'_\lambda \mid \lambda \in \mathrm{F}\}, . \rangle,$

es un espacio vectorial en el cuerpo$\mathcal{F}$. Además las condiciones binarias se cumplen:

(1) $(\varphi+\psi)\chi = \varphi\chi + \psi\chi$;
(2) $\chi\,(\varphi+\psi+) = \chi\varphi + \chi\psi$;
(3) $\lambda(\varphi\psi) = (\lambda\varphi)\psi = \varphi(\lambda\psi)$,

donde $\varphi, \psi, \chi \subset Hom(\mathcal{V},\mathcal{V})$ y $\lambda \in F$

Demuéstrese la igualdad (1). Si $\mathbf{x} \in V$, entonces

$$\big((\varphi+\psi)\chi\big)(\mathbf{x}) = (\varphi+\psi)\big(\chi\,(\mathbf{x})\big) = \varphi\big(\chi\,(\mathbf{x})\big)+\psi\big(\,\chi(\mathbf{x})\big) = (\varphi\chi)(\mathbf{x})+(\varphi\chi)(\mathbf{x}) = (\varphi\chi+\psi\chi)(\mathbf{x}),$$

es decir que resultándose en (1). De manera analógica, se demuestre (2).

Demostremos la primera de las igualdades de (3). Si $x \in V$, entonces

$$\big(\lambda(\varphi\psi)\big)(x) = \lambda\big((\varphi\psi)(x)\big) = \lambda\Big(\varphi\big(\psi(x)\big)\Big) = (\lambda\varphi)\big(\psi(x)\big) = \big((\lambda\varphi)\psi\big)(x),$$

Es decir $\lambda(\varphi\psi) = (\lambda\varphi)\psi$. de manera analógica, se demuestra la igualdad $(\lambda\varphi)\psi = \varphi(\psi)$■.

Isomorfismo del álgebra de operadores lineales y del álgebra matricial completa.

Sea $\mathfrak{U}$ y $\mathfrak{U}'$ algebras lineales en el cuerpo$\mathcal{F}$. La función Φ del álgebra $\mathfrak{U}$ en el algebra $\mathfrak{U}'$

Se llama *isomorfismo* si es inyectiva y respeta las operaciones principales del álgebra $\mathfrak{U}$, es decir
$\Phi(\mathbf{a}+\mathbf{b})=\Phi(\mathbf{a})+\Phi(\mathbf{b}), \Phi(\lambda\mathbf{a})=\lambda\Phi(\mathbf{a}), \Phi(\mathbf{ab})=\Phi(\mathbf{a})\Phi(\mathbf{b})$

Para todo $a, b \in V$ y todo $\lambda \in F$. Las álgebras $\mathfrak{U}$ **y** $\mathfrak{U}'$ son llamadas *isomorfas* si hay un isomorfismo del álgebra $\mathfrak{U}$ en el álgebra $\mathfrak{U}'$.

Se verifica sin dificultad que la relación de un isomorfismo de una colección cuales quiera del álgebra en el cuerpo $\mathcal{F}$ es una relación de equivalencia.

Ejemplo: el álgebra de números complejos

$\langle C, +, \{\omega_2 \mid \lambda \in \mathbf{R}\}, . \rangle$

es isomorfa en el álgebra de todas las matrices de la forma

$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ en $\mathcal{R}$:

$$\left\langle \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \boldsymbol{R} \right\}, +, \{\omega_2 \mid \lambda \in \boldsymbol{R}\}, . \right\rangle.$$

En este caso la correspondencia

$a + bi \rightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

Se establece por el isomorfismo de álgebras lineales consideradas.

Nótese $\mathfrak{M}(n, \mathcal{F})$ el álgebra matricial completa en $\mathcal{F}$

$\mathfrak{M}(n, \mathcal{F}) = \langle F^{n*n}, +, \{\omega_2 \mid \lambda \in \boldsymbol{F}\}, . \rangle$.

TEOREMA 3.3. Sea $\mathcal{V}$ un espacio vectorial de dimensión finita en el cuerpo $\mathcal{F}$ con una base fija $\mathbf{e}_1, \ldots, \boldsymbol{e}_{n.}$ *La función asignada a cada operador lineal* φ *del espacio* $\mathcal{V}$ *su matriz* $M(\varphi)$ *relativamente en la base fija constituye un isomorfismo del álgebra de operadores lineales End* $\mathcal{V}$ *en el álgebra matricial completa* $\mathfrak{M}(n, \mathcal{F})$.

Demostración. la correspondencia de $\varphi \rightarrow M(\varphi)$ es una función del conjunto *End* $\mathcal{V} = Hom(\mathcal{V}, \mathcal{V})$ en el conjunto $\mathrm{F}^{\mathrm{n*n}}$ de las matrices $n * n$. En virtud del TEOREMA 2.1, esta función es biyectiva. Además, respeta todas las operaciones principales del algebra *End* $\mathcal{V}$, es decir

(1) $M(\varphi + \psi) = M(\varphi) + M(\psi)$,
(2) $M(\lambda\varphi) = \lambda M(\varphi)$
(3) $M(\varphi\psi) = M(\varphi)M(\psi)$

Para todos $\varphi, \psi \in Hom(\mathcal{V}, \mathcal{V})$ y todo $\lambda \in F$. Las igualdades (1) y (2) están demostradas en el párrafo anterior.

Demuestrese en presente la igualdad (3). Sea $\mathbf{x} \in V$. Entonces

$(\varphi\psi)(\mathbf{x}) = \varphi(\psi(\mathbf{x}))$ Y según el TEOREMA 2.3,

$$M\big((\varphi\psi)(\mathbf{x})\big) = M\left(\varphi\big(\psi(\mathbf{x})\big)\right) = M(\varphi)M\big(\psi(\mathbf{x})\big) = [M(\varphi)M(\psi)]M(\mathbf{x}).$$

Así como, para todo vector $\mathbf{x} \in V$, en $\mathbf{a}$

$M\big((\varphi\psi)(\mathbf{x})\big) = [M(\varphi)M\psi]M(\mathbf{x})$.

Según el TEOREMA 2.4, se deduce la igualdad (3).

Por tanto, la aplicación considera es un isomorfismo del álgebra *End* $\mathcal{V}$ en el álgebra $\mathfrak{M}(n,\mathcal{F})$

Ejercicios.

1. Demostrar que la multiplicación de Cuaternion es asociativa
2. Demostrar que en el álgebra de Cuaterniones el sistemas de ecuación $\boldsymbol{i}x+\boldsymbol{i}y=\mathbf{e}, \quad \boldsymbol{k}x-\boldsymbol{e}y=\boldsymbol{i}$
   Admite una solución única, mientras que el sistema
   $xi+yj=e, \quad xk-ey=i$
   No tiene soluciones.
3. Sea $\mathbf{a}=a\mathbf{e}+\beta\mathbf{i}+y\mathbf{j}+\delta\boldsymbol{k}$ un cuaternion y $a^*=ae-\beta i-yj-\delta k$. mostrar que para todos los quaternion a,b en a

(a) $N(a)=aa^*=a^2+\beta^2+\gamma^2+\delta^2$;

(b) $N(ab)=N(a)N(b)$

(c) $(ab)^*=b^*a^*$.

4. Mostrar que existe un número infinito de cuaterniones satisfaciendo a la ecuación $x^2+e=0$
5. Sea $a=ae=\beta i+\gamma j+\delta k$ un quaternion cuales quiera. Verificar que los quaterniones $a\ y\ a^*$ son las raíces de la ecuación $x^2-2ax+N(a)e=0$.
6. Mostrar que si el cuaternion a no es un número real existe más que dos cuaternions cumplen a la ecuación $x^2=a$.
7. Demostrar que para los dos cuaternion a y b se tiene $(aa^*)(bb^*)=(ab)(a)^*$
   En conclusión, si cada uno de los números m,n es una suma de los cuadrados de cuatro enteros, entonces el producto mn es igualmente una suma de cuadarados de cuatro enteros.
8. Demostrar que en álgebra los cuaternions de cada una de las ecuaciones $ax=b, ya=b$ con $a\neq o$ admite una solución única.
9. Mostrar que el conjunto de todos los cuaterniones diferentes de zero constituye un grupo con respecto a la multiplicación.
10. Mostrar que ocho cuaterniones $\pm e,\pm i,\pm j,\pm k$ conforman un grupo multiplicativo (llamado *grupo cuaternionico).*
11. Sea $\mathfrak{U}$ un álgebra del rango n en el cuerpo $\mathcal{F}$. Mostrar que con $k>n$ todos k elementos del álgebra $\mathfrak{U}$ son linealmente dependientes en el cuerpo $\mathcal{F}$.
12. Siendo respectivamente $1,I,J,K$ las matrices complejas
    $\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}0&1\\-1&0\end{bmatrix},\begin{bmatrix}0&i\\i&0\end{bmatrix},\begin{bmatrix}i&0\\0&-i\end{bmatrix},$

    Donde $i=\sqrt{-1}$. mostrar que $I^2=J^2=K^2=-1, IJ=-JI=K, JK=-KJ=I, KI=-IK=J$.
13. Demostrar que el álgebra de matrices de la forma
    $\begin{bmatrix}a+\beta i&\gamma+\delta i\\-\gamma+\delta i&a-\beta i\end{bmatrix}$
    Con a,β,γ,δ reales y $i=\sqrt{-1}$ es isomorfa en álgebra de los cuaterniones en el cuerpo de números reales.

§ 4. Operadores invertibles.

Operadores invertibles sea φ un operador lineal del espacio vectorial $\mathcal{V}$ y ε un operador idéntico de este espacio. El operador φes llamado *invertible* si existe un operador lineal ψ del espacio $\mathcal{V}$ tal que

(1) $\varphi\psi=\varepsilon, \qquad \psi\varphi=\varepsilon.$

No hay un solo operador ψ que cumpla las condiciones (1).

De hecho, si el operador ψ_1 satisface a las condiciones $\varphi\psi_1 = \varepsilon, \psi_1\varphi = \varepsilon$, entonces
$\psi_1 = \psi_1\varepsilon = \psi_1(\varphi\psi) = (\psi_1\varphi)\psi = \varepsilon\psi = \psi,$
Es decir $\psi_1 = \psi$.

El operador lineal ψ que cumple las condiciones (1) se llama *operador inverso del operador* φ y se denota φ^{-1}.

TEOREMA 4.1. Sea φ *un operador lineal de un espacio vectorial* $\mathcal{V}$ *de dimensión finita* $\neq \{0\}$. *las condiciones siguientes son entonces equipotentes:*

(a) El operador φ *es invertible;*
(b) φ *es una función inyectiva de* $\mathcal{V}$ *en* $\mathcal{V}$;
(c) $ker\ \varphi = \{0\}$;
(d) Def $\varphi = 0$
(e) Rango $\varphi = dim\ \mathcal{V}$;
(f) *La matriz del operador* φ *relativamente en todas las bases del espacio* $\mathcal{V}$ *es inversible.*

Demostración. sea φ un operador inversible y ψ el operador inverso de φ. Demuéstrese que φ es injectivo, es decir que para todos $a, b \in V$ se deduce de $\varphi(a) = \varphi(b)$que $a = b$. de hecho, si $\varphi(a) = \varphi(b)$entonces

$$\psi\big(\varphi(a)\big) = \psi\big(\varphi(b)\big),\ (\psi\varphi)(a) = (\psi\varphi)(b), \varepsilon(a) = \varepsilon(b),\ a = b.$$

Además φ es una aplicación en V, es decir que para todos $a, \in V$
Se tiene una imagen anticipada. De hecho,

$$\varphi\big(\psi(a)\big) = (\varphi\psi)a = \varepsilon a = a,$$

Es decir qué $\varphi(a)$ es la imagen anticipada de a en la función φ.
Si φes una inyección, el vector nulo 0 posee una imagen anticipada única en la función φ, es decir $\ker\varphi = \{0\}$.
Si $\ker\varphi = \{0\}$, la dimensión del núcleo del operador φ es nula, es decir $\mathrm{def}\,\varphi = 0$.
Si $\mathrm{def}\,\varphi = 0$, entonces, según el TEOREMA 1.4, rango $\varphi = \dim\mathcal{V}$. Supóngase que el rango $\varphi = \dim\mathcal{V} = n$. Siendo $e_{1,\ \ldots\ ,}e_n$ la base fija del espacio $\mathcal{V}$.

Según el TEOREMA 2.6, el rango de la matriz $M(\varphi)$es igual al del operador φ y por tanto, el valor n. al igual las líneas de la matriz $M(\varphi)$ son linealmente independientes. Por lo tanto, según el TEOREMA 5.1, la matriz $M(\varphi)$ es inversible.
Supóngase que la matriz $M(\varphi)$es inversible y $\mathcal{B}$ y su matriz inversa, es decir

$M(\phi)B = E$ y $BM(\varphi) = E$.

Según el TEOREMA 2.1, existe un operador lineal ψ del espacio $\mathcal{V}$ tal que B sea la matriz del operador ψ relativamente en la base fija, es decir $B = M(\varphi)$. Además $M(\varepsilon) = E$, por tanto, $M(\varphi)M(\psi) = M(\varepsilon)$ y $M(\psi)M(\varphi) = M(\varepsilon)$.

En virtud del TEOREMA 3.3,$M(\varphi)M(\psi) = M(\varphi\psi)$ y $M(\psi)\,\big|\,M(\varphi) = M(\psi\varphi)$, al igual se ve
$M(\varphi\psi) = M(\varepsilon),\ M(\psi\varphi) = M(\varepsilon)$

Según el TEOREMA 2.1, se deducen las igualdades $\varphi\psi = \varepsilon$ y $\psi\varphi = \varepsilon$, es decir que el operador φ es inversible
■

Grupo lineal completo: según el TEOREMA 5.1, el conjunto de todas las matrices invertibles $n \times n$ en el cuerpo $\mathcal{F}$ es un grupo en relación a las operaciones de multiplicación y de inversión.

DEFINICIÓN: un grupo multiplicativo de todas las matrices invertibles $n \times n$ en el cuerpo $\mathcal{F}$ es llamado *grupo lineal completo de grado* n en el cuerpo $\mathcal{F}$ y se denota $GL(n, \mathcal{F})$.

Se ve fácilmente que todo operador invertible del espacio vectorial $\mathcal{V}$ es un isomorfismo de este espacio. Inversamente, todo automorfismo del espacio $\mathcal{V}$ es un operador inversible. El conjunto de todos los operadores inversibles de este espacio vectorial $\mathcal{V}$ es llamado $\mathrm{Aut}\,\mathcal{V}$.

Considérese el algebra $\langle \mathrm{Aut}\,\mathcal{V},\ .\ , {}^{-1}\rangle$, donde es una operación binaria de multiplicación de operadores inverso del operador dado; esta algebra será designada por el símbolo $\mathrm{Aut}\,\mathcal{V}$.

TEOREMA 4.2. Sea $\mathcal{V}$ un espacio vectorial en el cuerpo $\mathcal{F}$ el algebra $\mathrm{Aut}\,\mathcal{V}$ es entonces un grupo.

Demostración. el conjunto $\mathrm{Aut}\,\mathcal{V}$ de operadores inversibles del espacio $\mathcal{V}$es cerrado en relación y $^{-1}$. De hecho, si φes un operador inversible φ^{-1} e s entonces un operador inversible. Puesto que $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. ademas si φ y ψ son operadores inversibles , su producto es un operador lineal inversible, puesto que

$$(\varphi\psi)(\psi^{-1}\varphi^{-1}) = \varepsilon \quad \text{y} \quad ((\psi^{-1}\varphi^{-1})(\varphi\psi) = \varepsilon.$$

Según el TEOREMA 2.3, la multiplicación de operadores lineales es asociativa. El operador idéntico ε es inversible y es un elemento neutro en comparación a la multiplicación. Es decir que $\varphi\varepsilon = \varepsilon\varphi = \varphi$ para todo operador lineal φ. En conclusión para todo operador invertible φ se verifican las igualdades $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. al igual, las operaciones principales del algebra $Aut\ \mathcal{V}$ satisfacen a todos los oxiomas del grupo. Por tanto, esta algebra es un grupo. ■

TEROEMA 4.3. Sea $\mathcal{V}$ *un espacio vectorial de dimensión* $n \neq \{0\}$ *en el cuerpo* $\mathcal{F}$. El grupo $Aut\ \mathcal{V}$ es entonces isomorfo al grupo matricial lineal completo $GL(n, \mathcal{F}.)$

Demostración. considérese una función biyectiva

$\Phi: \mathrm{Aut}\,\mathcal{V} \to \mathrm{GL(n}, \mathcal{F}),$

Defina por la igualdad $\Phi(\varphi) = \mathrm{M}, \mathrm{donde}\ \mathrm{M}(\varphi)$ es la matriz del operador lineal φ relativamente en la base fija del espacio $\mathcal{V}$. Según el TEOREMA 3.3, para todos $\varphi, \psi \in Aut\ \mathcal{V}$

$$M(\varphi\psi) = M(\varphi)M(\psi).$$

Por tanto, para todos los operadores invertibles $\varphi, \psi\ en\ un\ \Phi(\varphi\psi) = \Phi(\varphi)\Phi(\psi)$. Según el TEOREMA 3.3.1, se deduce que Φ es un homomorfismo. Φ Es entonces un isomorfismo del grupo $Aut\ \mathcal{V}$ en el grupo $GL(n, \mathcal{F}.)$ ■

Ejercicios.

1. Sea φ, ψ los operadores lineales inversibles de un espacio vectorial. Demostrar que $\varphi\psi$ es un operador lineal inversible y $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1.}$
2. Mostrar que los operadores lineales φ, ψ de un espacio vectorial son inversibles si y sólo si los operadores $\varphi\psi$ y $\psi\varphi$ lo son.

3. Sea φ un operador inversible del espacio vectorial $\mathcal{V}$. Mostrar que φ es un isomorfismo de $\mathcal{V}$ en $\mathcal{V}$.
4. Sea φ, ψ los operadores lineales de un espacio vectorial $\mathcal{V}$ de dimensión finita. Mostrar que si $\varphi\psi$ es un operador idéntico del espacio $\mathcal{V}$,entonces φ y ψ son inversibles.
5. Sea φ, ψ los operadores lineales de un espacio vectorial. Mostrar que si $\operatorname{Ker}\varphi = \operatorname{Ker}\psi = \{0\}$ entonces $\operatorname{Ker}(\varphi\psi) = \{0\}$
6. Sea φ una función lineal del espacio vectorial $\mathcal{U}$ en el espacio vectorial $\mathcal{V}$ y ψ una función lineal de $\mathcal{V}$ en el espacio vectorial $\mathcal{W}$. Demostrar que si $\ker\varphi = \{0\}\, y\, \ker\psi = \{0'\}, entonces\, \ker(\psi\varphi) = \{0\}$.
7. Sea φ un operador inversible y ψ un operador lineal cuales quiera de un espacio vectorial de dimensión finita. Mostar que el rango $(\varphi\psi) = \operatorname{rango}(\psi\varphi) = \operatorname{rango}\psi$.
8. Demostrar que el operador lineal del espacio vectorial de dimensión finita $\mathcal{V}$ es inversible si y sólo si al transformarse cada sistema de vectores linealmente independiente del espacio $\mathcal{V}$es un sistema de vectores linealmente independientes de este espacio.
9. Sea $\mathcal{H}om(\mathcal{V},\mathcal{V})$ un espacio vectorial de todos los operadores lineales del espacio $\mathcal{V}$. Sea φun operador fijo y ψ un operador lineal cuales quiera del espacio $\mathcal{V}$. Demostrar que la función $\psi \to \varphi\psi$ es un operador lineal del espacio $\mathcal{H}om(\mathcal{V},\mathcal{V})$. Mostrar que el conjunto $\{\varphi\psi \mid \psi Hom(\mathcal{V},\mathcal{V})\}$ coincide con el conjunto de todos los operadores lineales del espacio vectorial $\mathcal{H}om(\mathcal{V},\mathcal{V})$ si φ es un operador invertible.

§ 5. Vectores propios y valores propios. Ecuaciones Características.

Vectores propios y valores propios: sea $\mathcal{V}$ un espacio vectorial en el cuerpo $\mathcal{F}$ y φ un operador lineal de este espacio.

DEFINICIÓN: un vector $a \in V$ es llamado *un vector propio del operador* φ si $a \neq 0$ y el vector $\varphi(a)$ es igual al producto de un escalar y del vector a.

El escalar $\lambda \in F$ llamado *valor propio del operador* φ si existe un vector a no nulo tal que $\varphi(a) = \lambda a$.

Si a es un vector propio del operador del operador φ, existe entonces un escalar $\lambda \in F$ único que cumple a la condición $\varphi(a) = \lambda a$. De hecho si $a \neq 0$ se deduce la igualdad $\lambda a = \lambda_1 a$ que $\lambda = \lambda_1$. al igual si $\varphi(a) = \lambda a$, se dice que el vector a es asociado a l valor propio λ.

Ejemplo:

1. Sea $\mathcal{V}$ un espacio vectorial $\neq \{0\}$en el cuerpo F y λ un escalar de elección fija. Defínase la función $\varphi: V \to V$, se plantea $\varphi(a) = \lambda a$ para todos $a \in V$ se ve sin duda que φ es un operador lineal del espacio V, se llama *operador homotético de continuidad* λ. El escalar λ es el valor propio del operador φ quien, además, es único. Todo vector no nulo del espacio V es un vector propio del operador φ asociado al valor propio λ.

2. Sea V un espacio vectorial de funciones reales en una variable definida en R e indefinidamente derivables; V es el espacio en el cuerpo de los números reales $\mathcal{R}$.
   Nótese $\frac{d}{dx}$ el operador de derivación asociado a cada elemento $f \in V$ se deriva $\frac{df}{dx}$. Se ve sin duda que el operador de derivación es un operador lineal del espacio V. Si $\lambda \in R$, la función $e^{\lambda x}$ es entonces el vector propio del operador de derivación, puesto que $\frac{de^{\lambda x}}{dx} = \lambda e^{\lambda x}$. al igual, todo número real es el valor propio del operador de derivación.

3. Sea $\mathcal{V}$ un espacio vectorial bidimensional en el cuerpo de los números reales $R, \mathcal{V} = \mathcal{R}^2$ y $a \in R$. Nótese φ_a el operador de rotación asignado a cada vector del espacio $\mathcal{V}$ un vector formado con un vector de salida un ángulo a. Se ve sin duda que φ_a es un operador lineal del espacio $\mathcal{V}$ que no cuenta con vectores propios si $a \neq k\pi$, donde k es un entero.

Nótese ε el operador idéntico Del espacio vectorial $\mathcal{V}$. Si φ es un operador lineal del espacio vectorial $\mathcal{V}$y λ un escalar arbitrario, $\lambda \in F$, se constata fácilmente que $\lambda\varepsilon - \varphi$ es un operador lineal del espacio $\mathcal{V}$.

PROPOSICION 5.1. Sea φ *un operador lineal del espacio vectorial* $\mathcal{V}$*y* λ *el valor propio de este operador. El conjunto de todos los vectores propios* φ*concinden con el conjunto* $\mathrm{Ker}(\lambda\varepsilon - \varphi) \setminus \{0\}$.

Demostración. según la definición del núcleo,

$$Ker\ (\lambda\varepsilon - \varphi) = \left\{x \in V \,\middle|\, (\lambda\varepsilon - \varphi)(x) = 0\right\}.$$

Si $a \in \ker(\lambda\varepsilon - \varphi) \setminus \{0\}$ entonces

$(\lambda\varepsilon - \varphi)(a) = 0,\ \ \lambda\varepsilon(a) - \varphi(a) = 0,\ \ \varphi(a) = \lambda a.$

Así todos los vectores no nulos del conjunto $Ker\ (\lambda\varepsilon - \varphi)$ es el vector propio del operador φ.

Sea b un vector propio cuales quiera del operador φ asociado en λ, es decir $\varphi(b) = \lambda b$, en este caso,

$$\lambda b - \varphi(b) = 0, \qquad \lambda\varepsilon b - \varphi(b) = 0, \quad (\lambda e - \varphi)(b) = 0.$$

Entonces, $b \in \ker(\lambda\varepsilon -), y\ como\ b \neq 0,$ entonces

$$b \in \ker(\ \lambda\varepsilon - \varphi) \setminus \{0\}. \blacksquare$$

Determinación de vectores propios de un operador lineal.

Sea $\mathcal{V}$ un espacio vectorial en el cuerpo F con una base fija $e_1, \ . \ . \ . \ . \ . \ ., e_n\ \varphi$ un operador de este espacio y $A = M(\varphi)$ la matriz del operador φrelativamente en la base fija, $A = \| a_{ik} \|$.

Para determinar los vectores propios del operador φ asociado a λ hacemos la búsqueda $\ker(\ \lambda\varepsilon - \varphi)$. Sea x un vector de V; posee en la base fija una colunma de cordenadas $\chi = M(x)$:

$$\chi = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Según el TEOREMA 2.3, las columnas de coordenadas del vector $(\lambda\varepsilon - \varphi)(x) es\ (\lambda E - A)\chi, es\ decir\ M(\lambda -)(x)) = (\lambda E - A). el\ vector\ x \in \mathrm{Ker}(\lambda\varepsilon - \varphi)$ si y sólo si

$(\mathrm{I})(\lambda\mathrm{E} - \mathrm{A})\chi = 0.$

La condición (I) está escrita en forma de un sistema lineal homogéneo por consecuencia a las variables $x_1, \ . \ . \ ., x_n$:

$$(\lambda - a_{11})x_1 - a_{12}x_2 - . \ . \ . - a_{1n}x_n = 0;$$
$$-a_{21}x_1 + (\lambda - a_{22})x_2 - \ . \ . \ . - a_{2n}x_n = 0;$$
$$. \ .$$

$$-a_{n1}x_1 - a_{n2}x_2 - \ldots + (\lambda - a_{nn})x_n = 0;$$

El vector $x \in V$es un vector propio del operador φ asociado al valor propio λ si y sólo si la línea de coordenadas $x_1, \ldots\ldots, x_n)$ del vector x es una solución no nula del sistema lineal homogéneo (1), téngase a bien demostrar la siguiente proposición .

PROPOSICION 5.2. Siendo φ*un operador lineal del espacio vectorial* $\mathcal{V}$ *con una base fija y* $M(\varphi) = A$ *la matriz del operador* φ*relativamente en la base fija. El vector x es un vector propio del operador* φ *asociado al valor propio* λ *si y sólo si la línea de coordenadas des vector* x *es una solución no nula del sistema (1).}*

Ecuación característica. Sea $\mathcal{V} = \mathcal{F}^n$ un espacio de vectores de columnas aritméticas de dimensión n en el cuerpo$\mathcal{F}$. Sea A la matriz $n \times n$ fija asociada en $\mathcal{F}$. Considérese la función $\psi: X \to AX$ para $X \in \mathcal{F}^n$. Se verifica fácilmente que ψ es un operador lineal del espacio $\mathcal{V}$.

DEFINICIÓN: sea A la matriz $n \times n$ asociada al cuerpo $\mathcal{F}$. El vector columna$X$ es llamado *vector propio de la matriz* A *si* X es un vector no nulo y AX puede estar representado en forma de un producto de un escalar y de un vector X, es decir su forma de $AX = \lambda X$.

λ En este caso es llamado *valor propio de la matriz* A*.*

Se denota sin duda que los vectores propios y los valores propios del operador lineal ψ son los vectores propios y los valores propios de la matriz A.

TEOREMA 5.3. Sea A *una matriz cuadrada del tipo* $n \times n$ en el cuerpo $\mathcal{F}$. El elemento λ *de* F es un valor propio de la matriz si y sólo si

(1) $\left|\lambda E - A\right| = 0$.

Demostración. el elemento $\lambda, \lambda \in F$, es un valor propio de la matriz A si y sólo si existe un vector columna $X_1 \in F^n$ no nulo tal que $AX_1 = \lambda X_1$ y, por lo tanto, $(\lambda E - A)X_1 = 0$. Dicho de otra manera, λ es 8un valor propio de la matriz A si y sólo si la ecuación

(2)$(A - \lambda E)X = 0$

Admite una solución no nula. La ecuación (2) puede estar considerada como la forma matricial de la escritura del sistema de n ecuaciones lineales a n variables con una matriz $(A - \lambda E)$ la ecuación (2) tiene una solución no nula si y sólo si el determinante de la matriz $(A - \lambda E)$ es nula. □

COROLARIO 5.4. *Un elemento* λ *del cuerpo* $\mathcal{F}$ *es un valor propio de la matriz* A *si y sólo si la matriz* $\lambda E - A$ *es irreversible.*

DEFINICIÓN*:* Sea A una matriz cuadrada del tipo $n \times n$ en el cuerpo$\mathcal{F}$. La ecuación $\left|\lambda E - A\right| = 0$ en variable λ es llamada *ecuación característica de la matriz* A

COROLARIO 5.5. Un escalar $\lambda \in F$ *es valor propio de la matriz cuadrada* A*(en* $\mathcal{F}$*) si y sólo si* λ *es una raíz de la ecuación característica de esta matriz.*

Ejemplo:

Sea $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$una matriz asociada al cuerpo del escalar $\mathcal{R}$. Entonces

$$\lambda E - A = \begin{bmatrix} \lambda - 1 & -1 \\ -2 & \lambda - 1 \end{bmatrix}$$

La ecuación

$\begin{vmatrix} \lambda-1 & -1 \\ -2 & \lambda-1 \end{vmatrix}$ = 0 ó $(\lambda-1\quad)^2-2=0$

Es la ecuación característica de la matriz A. sus raíces $\lambda_1 = 1 +$

$+\sqrt{2}$, $\lambda_2 = 1-\sqrt{2}$ son los valores propios de la matriz A.

PROPOSICION 5.6. Siendo A y B las matrices $n \times n$ *semejantes sobre el cuerpo de escalares*. $\mathcal{F}$. Entonces $|\lambda \mathrm{E}-\mathrm{A}| = |\lambda \mathrm{E}-\mathrm{B}|$ *y las ecuaciones de esas matrices características coinciden*.

Demostración. Puesto que A y B son semejantes, existe una matriz inversible T sobre $\mathcal{F}$ tal que $\mathrm{A}=\mathrm{T}^{-1}\mathrm{BT}$, por tanto;

$|\lambda\,\mathrm{E}-\mathrm{A}=\lambda\mathrm{E}-\mathrm{T}^1\,\mathrm{BT}=\mathrm{T}^1\,|\,(\lambda\mathrm{E}-\mathrm{B})\mathrm{T}$

Por lo tanto,

$|\lambda\mathrm{E}-\mathrm{A}| = |\mathrm{T}^{-1}||\lambda\mathrm{E}-\mathrm{B}\quad|\,|\mathrm{T}|.$

como $|\mathrm{T}^1||\mathrm{T}| = |\mathrm{T}^{-1}\mathrm{T}| = |\mathrm{E}| = 1, \text{tenemos} |\lambda\mathrm{E}-\mathrm{A}| =$

$=|\lambda\mathrm{E}-\mathrm{B}|$. Se deduce que las ecuaciones características

$|\lambda\mathrm{E}-\mathrm{A}|=0$ y $|\lambda\mathrm{E}-\mathrm{B}|=0$

De las matrices A y B coinciden. □

Definición. Sea φ un operador lineal del espacio vectorial $\mathcal{V}$
De dimensión finita $\neq \{\boldsymbol{O}\}$ y $M\,(\varphi)$ **.** Su matriz relativamente de una base cualesquiera. La ecuación, $|\lambda\mathrm{E}-\mathrm{M}(\varphi)|$= 0 *es llamada ecuación característica del operador* φ

Operadores lineales de espectro simple. Estudiemos los operadores de un espacio vectorial de dimensión n que posee n valores propios diferentes.

TEOREMA 5.7 Si los vectores propios $\boldsymbol{a_1}, \ldots, \boldsymbol{a_m}$ *del operador lineal, correspondiente a valores propios diferentes, el sistema* $\boldsymbol{a_1}, \ldots, \boldsymbol{a_m}$ *es entonces independiente.*

DEMOSTRACIÓN. sea(φ) un operador lineal del espacio vectorial $\mathcal{V}$ y $\boldsymbol{a_1}, \ldots, \boldsymbol{a_m}$ sus vectores propios asociados a diferentes valores propios, es decir

$(1)\ \varphi(\boldsymbol{a}_1) = \lambda_1\boldsymbol{a}_{1.}, \ldots, \varphi(\boldsymbol{a}_m) = \lambda_m\,\boldsymbol{a}_m$

y

$(2)\lambda_i \neq \lambda_k$ a $i \neq k.$

La demostración se efectúa por la recurrencia sobre el número m.puesto que todo vector propio se diferencia del vector nulo, el TEOREMA es verdadero para $m = 1$. Suponiendo que el TEOREMA es verdadero para m vectores. Debemos demostrar que para todos

$\alpha_1, \dots, \alpha_m \in F$ Se cumple la igualdad

(3) $\alpha_1 \boldsymbol{\alpha}_1 + \dots + a_{\boldsymbol{m}} \boldsymbol{a}_{\boldsymbol{m}} = \boldsymbol{O}$

Las igualdades

(4) $\alpha_1 = O, \dots, a_{\boldsymbol{m}} = O.$

φ que es un operador lineal seguido de (3) la igualdad $\alpha_1 \varphi(a_1) + \dots$

$\dots + \alpha_m \varphi(\boldsymbol{a}_m) = \mathbf{0}$ y, en virtud de, (1), tenemos

(5) $\alpha_1 \lambda_1 \boldsymbol{a}_{\mathbf{1}} + \dots + a_m \lambda_m \boldsymbol{a}_m = \mathbf{0}.$

Añádase dos miembros de igualdad (5) las partes correspondientes de la igualdad (3) multiplicadas por $(-\lambda_m)$, entonces

(6) $\alpha_1 (\lambda_1 - \lambda_m) \boldsymbol{a}_{\mathbf{1}} + \dots + a_{m-1} (\lambda_{m-1} - \lambda_m) \alpha_{m-1} = 0.$

Según la hipótesis de inducción, el sistema de vectores propios $\boldsymbol{a}_{\mathbf{1}}, \dots, \boldsymbol{a}_{\boldsymbol{m-1}}$ es linealmente independiente. Así que se Deduce de (6) las igualdades

$\alpha_1 (\lambda_1 - \lambda_m) = 0, \dots, a_{m-1} (\lambda_{m-1} - \lambda_m) = 0.$

Debido a (2) tenemos que

(7) $\alpha_1 = 0, \dots, a_{m-1} = 0.$

En virtud de (3) y (7) $a_m \boldsymbol{a}_m = 0,$ además, $\boldsymbol{a}_m \neq \mathbf{0}$; por lo tanto, $\boldsymbol{a}_m = 0.$

Se ha demostrado entonces que dé (3) se deduce (4), es decir que el sistema $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ es linealmente independiente.□

DEFINICIÓN: El operador lineal de un espacio vectorial de dimensión n $(n > 0)$

Que posee n valores propios diferentes, es llamado *operador de espectro simple*; la serie de todos los valores propios de un operador es llamada *espectro del operador.*

PROPOSICIÓN 5.8 sea φ *un operador lineal del espacio vectorial* $\mathcal{V}$ *de dimencion* n *del espectro simple* $\{\lambda_1, \dots, \lambda_n\}$. *Sean* $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ *los vectores propios del operador* φ *asociados respectivamente* a $\lambda_1, \dots, \lambda_n$. El sistema, $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ *es entonces una base del espacio* $\mathcal{V}$.

Demostración. Por hipótesis, el espectro $\lambda_1, \dots, \lambda_n$. Del operador φ está compuesto de escalares diferentes dos a dos. Debido al TEOREMA 5.7, se deduce que el sistema de vectores propios $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ es

linealmente independiente. Según el corolario 7.3.4 se deduce que el sistema $\boldsymbol{e_1}, \ldots, \boldsymbol{e_n}$ es una base del espacio $\mathcal{V}$. □

TEOREMA 5.9. Sea φ un operador lineal del espacoio vectorial $\mathcal{V}$ de dimensión n en espectro simple $\boldsymbol{\lambda_1}, \ldots, \boldsymbol{\lambda_n}$ y $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ de vectores propios del operador φ asociados respectivamente a los valores propios $\boldsymbol{\lambda_1}, \ldots, \boldsymbol{\lambda_n}$. La matriz diagonal.

$$(1)\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

Es entonces un matriz del operador φ relativamente en la base $\boldsymbol{e_1}, \ldots, \boldsymbol{e_n}$ y para todo vector $\mathbf{x} = x_1\boldsymbol{e}_1 + \ldots + x_n\boldsymbol{e}_n$ del espacio $\mathcal{V}$

(2) $\varphi(\mathbf{x}) = \boldsymbol{\lambda_1 x_1 e_1} + \ldots + \boldsymbol{\lambda_n x_n e_n}$.

Demostración Por hipótesis,

(3) $\varphi(e_1) = \lambda_1 x_1 e_1 + \ldots + \lambda_n x_n e_n$.

Esas igualdades muestran que la matriz diagonal (1) es una matriz del operador φ relativamente a la base $\mathbf{e}_1, \ldots, \mathbf{e_n}$ se deduce, si $\mathbf{x} \in$ v y $\mathbf{x} = x_1 e_1 + \ldots + x_n\, \varphi(e_n)$,

Debido a la linealidad del operador φ , tenemos $\varphi(\mathbf{x})\mathbf{x}_1\varphi(e_1) + \ldots + \mathbf{x}_n\varphi(e_n)$. En virtud de (3), se deducen las igualdades (2). □

Condiciones de similitud de una matriz a una matriz diagonal.

TEOREMA 5.10 Sea A una matriz $n \times n$ sobre el cuerpo $\mathcal{F}$ que posee n vectores propios linealmente independientes y T la matriz cuyas columnas son vectores propios linealmente independientes de la matriz A . La matriz $T^{-1}AT$ es entonces la diagonal, y los elementos de su diagonal principal son los valores propios de la matriz A.

DEMOSTRACIÓN. Sea

$\mathrm{x}_1, \ldots, \mathrm{x}_n$

Los vectores propios linealmente independiente de la matriz A asociados respectivamnete a $\boldsymbol{\lambda_1}, \ldots, \boldsymbol{\lambda_n}$ es decir,

$AX_1 = \lambda_1 x_1, \ldots, AX_n = \lambda_n x_n$.

Nótese T una matriz tal, de manera que $T^i = \mathrm{X}_i$ para $i = 1, \ldots, n$,
Es decir

$T = [\mathrm{x}_1, \ldots, \mathrm{x}_n]$.

Como las columnas de la matriz T son linealmente independientes, ésta última es inversible. De la definición del producto de las matrices,
Deducimos que
$AT = [\mathrm{AX}_1, \ldots, \mathrm{AX}_n]$;

Donde debido a (1), tenemos

$$AT = [\lambda_1 \mathrm{x}_1, \ldots, \lambda_n \mathrm{x}_n] = [\mathrm{x}_1, \ldots, \mathrm{x}_n] \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} =$$

$$T = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

Obtenemos entonces

$$T^{-1} AT = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}. \square$$

TEOREMA 5..11. *Si una matriz cuadrada A de orden n es semejante al cuerpo $\mathcal{F}$ de una matriz diagonal, entonces la matriz A tiene n verctores propios linealmente independientes.*

DEMOSTRACIÓN. Supóngase que la matriz A es semejante a los cuerpos $\mathcal{F}$ de una matriz diagonal, es decir que existe una matriz inversible T tal que

$$(1) \quad T^{-1} AT = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

Con $\lambda_1, \ldots, \lambda_n \in F$. Multipliquemos a la izquierda los dos miembros de la igualdad (1) para T, tenemos entonces

$$AT = T \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

Por lo tanto,
$[AT^1, \ldots, AT^m] = [\lambda_1 T^1, \ldots \lambda_n T^m]$,
Y por lo tanto
$AT^1 = \lambda_1 T^1, \ldots, \mathrm{A}T^m = \lambda_n T^n$,

Dicho de otra manera las columnas $T^1, \ldots, T^n$ de la matriz T son vectores propios asociados respectivamente a $\lambda_1, \ldots, \lambda_n$. Como la matriz T es inversible, sus columnas son linealmente independientes (según el TEOREMA 5.1). □

Ejercicios.

1. Buscar los vectores propios y los valores propios de las matrices siguientes en el cuerpo de números racionales:

   (a) $\begin{bmatrix}01\\10\end{bmatrix}$; (b) $\begin{bmatrix}1\ 2\\3\ 4\end{bmatrix}$; (c) $\begin{bmatrix}-1\ \ 1\\\ \ 1\ \ 1\end{bmatrix}$.

2. Sea a un número real no nulo. Mostar que la matriz $\begin{bmatrix}\ 0\ \ a\\-a\ \ 0\end{bmatrix}$

   No posee los valores propios reales.

3. Sea a un número real diferente de cero. Buscar los valores propios y los vectores propios en el cuerpo de números complejos de la matriz
   $\begin{bmatrix}\cos a\ \ \sin\ a\\-\sin a\ \cos a\end{bmatrix}$.
4. Buscar los vectores propios y los valores propios sobre el cuerpo de números complejos de las siguientes matrices.
   (a) $\begin{bmatrix}0\ 0\ 1\\0\ 1\ 0\\1\ 0\ 0\end{bmatrix}$; (b) $\begin{bmatrix}0\ 0\ 0\\1\ 0\ 1\\0\ 1\ 0\end{bmatrix}$; (c) $\begin{bmatrix}1 & \ \ 2\\2 & -2\end{bmatrix}$; (d) $\begin{bmatrix}-1 & -\ 2i\\2\ i & -2\end{bmatrix}$.

5. Sea $A=\begin{bmatrix}a\ \beta\\\gamma\ \delta\end{bmatrix}$ una matriz en el cuerpo $\mathcal{F}$. Mostrar que el escalar $\lambda \in F$ es un valor propio de la matriz A cuando $\lambda^{\mathbf{2}} - (a\ +\delta\ )\lambda + (a\delta\ -\beta\gamma) = 0$.
6. Demostrar que los números reales son los valores propios de una matriz real simétrica.
7. Sea A una matriz cuadrada. Mostrar que la matriz transpuesta ${}^{t}A$ posee los mismos valores propios que la matriz A .
8. Mostrar que los valores propios de una matriz diagonal son sus elementos diagonales.
9. demostrar que los valores propios de una matriz triangular son sus elementos diagonales.
10. demostrar que todos los valores propios de una matriz cuadrada A son diferentes de cero, si y solo si la matriz A es inversible.
11. Sea A una matriz cuadrada y k todo entero positivo. Demostrar que si λ es es un valor propio de matriz A, $\lambda^{\mathcal{R}}$ es entonces un valor propio de matriz $\mathrm{A}^{\mathcal{R}}$.
12. Al conocerse los valores propios de una matriz invertible A , buscar los valores propios de la matriz A^{-1}.
13. Sea λ el valor propio de una matriz inversible A . Demostrar que λ^{n} es un valor propio de la matriz A^{n} para todo n entero.
14. Sea A una matriz cuadrada en el cuerpo $\mathcal{F}$:

    $f(\lambda) = a_0\ +\ a_1\lambda\ +\ .\ .\ .\ \ +a_m\lambda^m$, donde $a_0\,, a_1,\ \ .\ .\ ., a_m \in c$,

    $f(\mathrm{A}) = a_0\,E\ +a_1\mathrm{A}+\ .\ .\ .+a_m\,A^m$ (E es la matriz unitaria).

    Demostrar que si λ es un valor propio de la matriz A , entonces $f(\lambda)$ es un valor propio de la matriz $f(\mathrm{A})$. Mostrar que todo vector propio de la matriz (A) es un valor propio de la Matriz $f(\mathrm{A})$.

    15. Sea A, B matrices cuadradas $n \times n$ en el cuerpo F , siendo la matriz A inversible. Demostrar que las matrices A, B y B, A corresponden a una misma ecuación característica.
    16. buscar la matriz diagonal semejante al cuerpo de los números racionales:

(a) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$; (c) $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.

17. buscar la matriz diagonal semejante al cuerpo de números reales de la matriz:

(a) $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$; (b) $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$. (c) $\begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$.

18. buscar la matriz diagonal semejante al cuerpo de números complejos de la matriz $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

19. Sea a un número real no entero múltiplo de π. Demostrar que la matriz
$\begin{bmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{bmatrix}$ No es semejante a la matriz diagonal real.

20. muestra que toda matriz 2×2 real, cuyo determinante es negativo es semejante a la matriz diagonal real.

21. Sea $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$. Una matriz en el cuerpo F y $a \neq 0$. Demostrar que la matriz A no es semejante a la matriz diagonal.

22. Demuestra que dos matrices diagonales son semejantes si y solo si ellas son diferentes únicamente por el orden de disposición de los elementos diagonales.
23. Sea A una matriz semejante a la matriz diagonal. Demostrar que la matriz A^n es semejante a la matriz diagonal para todo entero positivo.
24. Buscar todas las matrices cuadradas de segundo orden en el cuerpo de los valores propios 1 y -1 .

CAPITULO IX
SISTEMA DE DESIGUALDADES LINEALES

§ 1. Sistema de desigualdades lineales.

Nociones elementales. El sistema de la forma

(1) $a_{i1}x_1 + \ldots + a_{in}x_n \leqslant \gamma_i \quad (i = 1, \ldots, m)$,

O $a_i \in \mathbf{R}, \gamma_i \in \mathbf{R}$, es llamado *sistemas de desigualdades lineales.*

Plantéese

$a_{i1}, \ldots, a_{in} \qquad (i = 1, \ldots, m).$

El sistema (1) puede ser escrito bajo la *forma vectorial:*

(2) $a_i \, x \leqslant \gamma_i \quad (i = 1, \ldots, m)$,

O $x = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_m \end{bmatrix}$.

Designamos para A la matriz compuesta por los coeficientes del sistema (1):

$A = \begin{bmatrix} a_{11} \ldots & a_{1n} \\ a_{m1} \ldots & a_{1m} \end{bmatrix}$.

El sistema (1) puedes ser escrito bajo la *forma matricial:*

(3)$A\mathrm{x} \times \leqslant \mathrm{c}, \quad \mathrm{o} \quad \mathrm{c} = \begin{bmatrix} \gamma_1 \\ \cdot \\ \cdot \\ \cdot \\ \gamma_n \end{bmatrix}$.

Sea $\mathcal{R}^n$ el espacio aritmetico de dimensión n en el cuerpo de numeros reales $\mathcal{R}$ y $\mathbf{R^n}$ su conjunto de base.

El vector $\mathbf{R^n}$ de las coordenadas $\xi_1, \ldots, \xi_n$ es llamado solución del sistema

(1) Si

$a_{i1}\xi_1 + a_{in}\xi_n \leqslant \gamma_i \qquad (i=1, \ldots, n).$

El sistema (1) se dice compatible si admite al menos una solución.

El sistema (1) se llama incompatible si no admite soluciones.

El vector $(\xi_1, \ldots, \xi_n) \in \mathbf{R}^n$ dicho *no negativo* si$\xi_n \geqslant$ Para $i = 1, \ldots, n$. Un vector no negativo es llamado positivo si al menos una de sus coordenadas es positiva.

La desigualdad

(4) $\beta_1 x_1 + \ldots + \beta_n x_n \leqslant \gamma$

Se llama *implicación del sistema* (1) si cada solución del sistema (1) es una solución de desigualdad (4).

Desigualdad de la forma

$(5)\ (\lambda_1 \mathbf{a_1} + \ldots + \lambda_m \mathbf{a_1})\ \mathbf{x} \leqslant \boldsymbol{\lambda_1}\, \boldsymbol{\gamma_1} + \ldots + \lambda_m \gamma_m,$

Donde $\lambda_1 \geqslant 0$, es llamado combinación lineal no negativa de desigualdades del sistema (2).

PROPOSICIÓN 1.1 *cualquier combinación lineal no negativa de desigualdades del sistema (2) es una implicación de ese sistema.*

D e m o s t r a c i ó n. Plantéese que la desigualdad (5) es una combinación lineal no negativa de desigualdades del sistema (2). Sea $\xi \in \mathbf{R}^n$ una solución cualquiera del sistema (2),

(6) $\mathbf{a}_i \boldsymbol{\xi} \leqslant \boldsymbol{\gamma_i} \qquad (i = 1, \ldots, m).$

Al multiplicar la $i - \acute{e}sima$ desigualdad de (6) por $\boldsymbol{\lambda_i}$ **para** $i = 1, \ldots, m$

Y al sumar esas desigualdades, entonces tenemos

$\lambda_1 \mathrm{a}_1 + \ldots + \lambda_m \mathrm{a}_m\, \xi \leqslant \lambda_i \gamma_1 + \ldots + \lambda_m \gamma_m$.

Entonces, la desigualdad (5) es la implicación del sistema (2).□

Sistema homogéneo de desigualdades lineales y conos convexos.

Sea $\mathcal{V}$ un espacio vectorial aritmético en el cuerpo vectorial de números reales $\mathcal{R}$, $\mathcal{V} = \mathcal{R}^n$ y c de vectores del espacio $\mathcal{V}$.

El sistema

$(1) \quad \mathrm{a}_i\, \mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m)$

se llama *sistema de desigualdad homogénea.*

DEFINICIÓN. Un conjunto de vectores no vacío del espacio vectorial $\mathcal{V}$,

cerrado en relación a la suma y multiplicación para escalares no negativos
(Números reales no negativos) es llamado cono *convexo del espacio* $\mathcal{V}$.

E j e m p l o s. 1. Sea $\mathbf{a} \in \mathbf{R}^n$, $\mathbf{a} \neq 0$. el conjunto

$\{\lambda \mathbf{a} | \ \lambda \geqslant 0, \lambda \in \mathbf{R}\}$

Es uno cono convexo del espacio $\mathcal{R}^n$. Este cono es llamado semirrecta, generado por el vector $\mathbf{a}$.

2. El conjunto de todas las combinaciones no negativas del sistema de vectores $a_1, \ldots, a_m$ del espacio $\mathcal{R}^n$ es un cono convexo de este espacio; se le denotará $L^+(a_1, \ldots, a_m)$.

3. Sea $\mathcal{V} = \mathcal{R}^n, \mathcal{L}$ que es un sub-espacio del espacio $\mathcal{V}$ y L su conjunto de base. Entonces, L es un cono convexo del espacio $\mathcal{V}$.

4. El conjunto de todas las soluciones negativas de un sistema de desigualdades lineales homogéneas (1) es un cono convexo del espacio $\mathcal{V}$.

5. Sea $\mathbf{a} \in \mathbf{R}^n$, $\mathbf{a} \neq \mathbf{0}$. El conjunto de todas las soluciones de desigualdades $a\,x \leqslant 0$
Es un cono convexo del espacio $\mathcal{V}$. Este cono es llamado sub- espacio del espacio $\mathcal{V}$ definido por el vector **a.**

PROPOSICIÓN 1.2 *Un conjunto de todas las soluciones del sistema lineal homogéneo* (1) *es un cono convexo de un espacio vectorial* $\mathcal{V}$*.*

La demostración de esta proposición se deja en manos del lector.

COROLARIO 1.3. ***Si*** $a_1, \ldots, a_m$ *son vectores no nulos, entonces el cono de todas las soluciones del sistema lineal homogéneo (1) es una intersección de* m *sub- espacio del espacio* $\mathcal{V}$*definido por los vectores* $a_1, \ldots, a_m$.

Implicación de un sistema homogéneo de desigualdades lineales. Para demostrar el TEOREMA de Minkowski, necesitamos dos lemas.

Lema 1.4 *Si*

(3) $\mathbf{b} \notin L(a_1, \ldots, a_m)$,

Entonces la desigualdad

(2) $\mathbf{bx} \leqslant 0$

No es una implicación del sistema

(1) $a_i \mathbf{x} \leqslant 0 \quad (\ i = 1, \ \ldots, m)$.

Demostración. El grado del sistema de vectores $a_1, \ldots, a_m$ Se denotará r. Supóngase que se cumple la condición (3),

Entonces.

(4) grado $(a_1, \ldots, a_m\ \} + 1 = r + 1$.

Sea

$a_i = (a_{i1}, \ldots, a_{in}) \quad (\ i = 1, \ \ldots, m)$

$\mathbf{b} = (\beta_1, \ldots, \beta_n)$.

Consideremos el sistema de ecuaciones lineales

$a_{11} x_1 + \ldots + a_1 x_n = 0,$

. . . . . .

(5) $a_{m1} x_1 + \ldots + a_{mn} x_n = 0,$

$\beta_1 x_1 + \ldots + \beta_n x_n = 1.$

Sobre la base de (4) se concluye que el grado de matrices fundamentales y completas del sistema (5) vale $r+1$. Por lo tanto, el sistema (5) es compatible. En consecuencia existe un vector ξ tal que

$\mathrm{a}_i\,\xi =$

$$0(\ \ i=1,\ \ldots,m)$$

$\mathbf{b}\xi = 1$

El vector ξ es la solución del sistema (1) que no satisface a (2). Entonces, la desigualdad (2) no es una implicación del sistema (1).□

COROLARIO 1.5 si la desigualdad (2) es la implicación del sistema (1),

Entonces

$\mathbf{b} \in L(\mathbf{a}_1,\ \ldots\ ,\mathbf{a}_m)$.

Según la ley de contraposición esta afirmación es equivalente al lema 1.4.

LEMA 1.6 *Sea la desigualdad*

(2) $\mathbf{cx} \leqslant 0$

Una implicación del sistema

(1) $\mathrm{a}_i\mathbf{x} \leqslant 0 \quad (\ \ i=1,\ \ldots,m)$.

y

(2) $\mathbf{c} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\,\mathrm{a}_{m-1} + \ \lambda_m\mathbf{a}_m$.

$$\lambda_1,\ \ldots\ ,\lambda_{m-1} \geqslant 0, \lambda_m \leqslant 0$$

Entonces, la desigualdad (2) es una implicación del sistema

(4) $\mathrm{a}_i\mathbf{x} \leqslant 0 \qquad (\ \ i=1,\ \ldots,m-1).$

Demostración. Considérese el sistema

(I) $\mathrm{a}_i\mathbf{x} \leqslant 0,\ \ \ldots,\mathrm{a}_{m-1}{}^{\mathbf{x}} \leqslant 0,\ \ (-\mathbf{a}_m)\,\mathbf{x} \leqslant 0$.

El vector $\mathbf{c}$ en virtud de (3), es una combinación lineal no negativa de los vectores $\mathbf{a}_1,\ \ldots,\mathrm{a}_{m-1}$, $(-\mathbf{a}_m)$,

(II) $\mathbf{c} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\,\mathbf{a}_{m-1} + \ (-\lambda_m)(-\mathbf{a}_m)$.

En virtud de la proposición 1.1, se deduce que (2) es una implicación del Sistema (II):

(5) $(\mathrm{II}) \rightarrow (2)$.

Demostremos que cualquier solución del sistema ξ (4) es una solución de la desigualdad (2). Dos casos son posible: $\mathbf{a}_m\,\xi \leqslant 0$ ó $(-\mathbf{a}_m)\,\xi \leqslant 0$, entonces ξ es una solución del sistema (1) y, por consiguiente, por hipótesis, ξ es una solución de la desigualdad (2). Si, por el contrario,

$\mathbf{a}_m\xi \leqslant 0$, entonces ξ es una solución del sistema (1´); por consiguiente, debido a (4), es igualmente una solución de desigualdad (2).en definitivo cualquier solución de (4) es una solución de la desigualdad (2). □

TEOREMA de Minkowski. En teoría de desigualdades lineales uno de los TEOREMAs esenciales es el siguiente.

TEOREMA 1.7 . Sea la desigualdad

$(2)\ \mathbf{bx} \leqslant 0$

Considerado como una implicación del sistema

(1) $\mathrm{a}_i\mathbf{x} \leqslant 0 \qquad (\ i = 1,\ \ldots, m)$.

Entonces, $\mathbf{b} \in \mathrm{L}^{+}\ (\mathbf{a}_1,\ \ldots,\ \mathbf{a}_m)$.

(1) D e m o s t r a c i ó n *) (conducta por recurrencia sobre m). El TEOREMA es verdadero para $m = 1$. En efecto, plantéese $\mathbf{b} \neq \mathbf{0}$**,** por hipótesis, la desigualdad $\mathbf{bx} \leqslant 0$ es la implicación de la desigualdad $\mathbf{a}_1\mathbf{x} \leqslant 0$. Según el corolario 1.5 , $\mathbf{b} = \lambda\mathbf{a}_1$, donde $\boldsymbol{\lambda} \in \mathbf{R}$. Como $\mathbf{b} \neq \mathbf{0}$**,** tenemos $\lambda \neq 0,\ \mathbf{a}_1 \neq 0$ y $\mathbf{a}_1\,\mathbf{a}_1 > 0$. Por tanto el vector $(-\mathbf{a}_1)$ es una solución de la desigualdad $\mathbf{a}_1\mathbf{x} \leqslant 0$ y por hipotesis, una solución de desigualdad (2) , es decir $\lambda\mathbf{a}_1(-\mathbf{a}_1) \leqslant 0$, por lo tanto, $\lambda > 0$. El TEOREMA es aparentemente verdadero para $\mathbf{b} = \mathbf{0}$ **.**

Supóngase que el TEOREMA se verifica cuando el sistema está compuesto de $m - 1$ desigualdades. Dado que $(\mathbf{1}) \rightarrow (\mathbf{2})$, debido al corolario 1.5, $\mathbf{b} \in \mathrm{L}\,(\mathbf{a}_1,\ \ldots,\ \mathbf{a}_m)$. Entre las representaciones del vector $\mathbf{b}$ existe una representación donde el número de coeficientes no negativos es el más grande. Sea

$$\mathbf{b} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_m\,\mathbf{a}_m$$

Una de esas representaciones. Sea s el número de coeficientes no negativo en (3) , $s \leqslant m$. Debemos demostrar que $s = m$. Plantéese que

$$(4)\ s < m.$$

Por convención, los coeficientes $\lambda_1\ ,\ \ldots,\lambda_s$ no son negativos. Considérese el vector

$$\mathbf{c} = \sum_{\mathbf{1} \leqslant i \leqslant s} \boldsymbol{\lambda_i}\mathbf{a_i} + \boldsymbol{\lambda_m}\mathbf{a_m};$$

Entonces,

$$(\mathbf{5})\ \mathbf{b} - \mathbf{c} = \sum_{s < \mathcal{R} < m} \boldsymbol{\lambda_{\mathcal{R}}}\mathbf{a_{\mathcal{R}}}\ .$$

Sea M un conjunto de todas las soluciones del sistema (1) y ξ un vector cualquiera de M, entonces $\mathbf{a_{\mathcal{R}}}\xi \leqslant 0$ y $\boldsymbol{\lambda_{\mathcal{R}}}\,(\,\mathbf{a_{\mathcal{R}}}\xi) \geqslant 0$ si s y $< k <$
$< m$; Por consiguiente

$$(6)(\mathbf{b} - \mathbf{c})\xi = \sum_{s < \mathcal{R} < m} \boldsymbol{\lambda_{\mathcal{R}}}\mathbf{a_{\mathcal{R}}} \geqslant 0.$$

*)La demostración figura en la obra de S. N Tchernikov TEOREMAs fundamentales de la teoria de desigualdades lineales´´(С .Н ОбЧерников основных теоремах теореии линейных нераВенстВ´´ .Сибирск. матем. ж ., 1964, **N**° 5).

Además, por hipótesis $\mathbf{b}\xi \leqslant 0$; por lo tanto,

(7) $\mathbf{c}\xi + (\mathbf{b} - \mathbf{c})\xi \leqslant 0.$

Sobre la base de (6) y (7) se concluye que $\mathbf{c}\xi \leqslant 0$ para todo ξde M , es decir que la desigualdad de $\mathbf{cx} \leqslant 0$ es una implicación del sistema (1).

Según el lema 1.6, se deduce que la igualdad $\mathbf{cx} \leqslant 0$ es una implicación del sistema

$\mathbf{a_i}\mathbf{x} \leqslant 0 \qquad (\ i = 1,\ \ldots, m-1)$,

Compuesto de $m - 1$ desigualdades. Según la hipótesis de recurrencia,

$\mathbf{c} \in L^{+}\ (\mathbf{a}_1,\ \ldots,\ \mathbf{a}_{m-1})$, es decir $\mathbf{c}$ puede ser representado bajo la forma de

(8) $\mathbf{c}\,\boldsymbol{\lambda}_1\mathbf{a}_1+\ldots+\boldsymbol{\gamma}_{m-1}\,\mathbf{a}_{m-1}$, donde $\boldsymbol{\gamma}_1,\ldots,\boldsymbol{\gamma}_{m-1}\geqslant 0$.

Debido a (5) y (8)

$$\sum_{1\leqslant i\leqslant s}\gamma_i\mathbf{a}_i+\sum_{s<\mathcal{R}<m}(\gamma_{\mathcal{R}}+\lambda_{\mathcal{R}})\,\mathbf{a}_{\mathcal{R}}+\mathbf{0}.\,\mathbf{a}_m.$$

En esta representación del vector $\mathbf{b}$ el número de coeficientes no negativos es superior a s. Eso contradice la hipótesis de la representación (3), que el vector $\mathbf{b}$ tiene el más grande número de coeficientes no negativos. Se llegó a una contradicción al admitir que $s<m$. Entonces este caso es imposible. Por consiguiente, $s=m$, es decir (3) es la representación buscada del vector $\mathbf{b}$ en la forma de una combinación no negativa de vectores $\mathbf{a}_1,\ldots,\mathbf{a}_m$. □

Criterio de incompatibilidades de un sistema de desigualdades lineales. Pásese al estudio de sistemas de desigualdades lineales homogéneas.

TEOREMA 1.8. *El sistema de desigualdades*

(1) $\mathbf{a}_i\mathbf{x}\leqslant\gamma_i\qquad(i=1,\ldots,m)$

Es incompatible si y solo si existen números reales $\lambda_1,\ldots,\lambda_m$ *que cumplen las condiciones*

(2)
$$\begin{aligned}&\boldsymbol{\lambda}_1\mathbf{a}_1+\ldots+\boldsymbol{\gamma}_m\,\mathbf{a}_m=\mathbf{0}\\&\boldsymbol{\lambda}_1\,\boldsymbol{\gamma}_1+\ldots+\boldsymbol{\lambda}_m\,\boldsymbol{\gamma}_m<\mathbf{0}\end{aligned}\qquad(\boldsymbol{\lambda}_1\geqslant 0,\ \ldots,\ \boldsymbol{\lambda}_m\geqslant 0)$$

D e m o s t r a c i ó n. Supóngase que el sistema (1) es incompatible y demostremos que existen los números reales que cumplen las condiciones (2). Sea

(3) $\mathbf{a}_i=(\mathrm{a}_{i1},\ldots,\mathrm{a}_{in})\qquad(i=1,\ldots,m).$

Considérese un sistema de desigualdades homogéneo

(4) $\mathrm{a}_{i1}x_1+\ldots+\mathrm{a}_{in}x_n-\gamma_i\,x_{n+1}\leqslant 0\qquad(i=1,\ldots,m)$

A las variables $x_1,\ldots,x_n,x_{n+1}.\leqslant 0$ La desigualdad

5) $0.x_1+\ldots+0.x_n+x_{n+1}\leqslant 0$

Es una implicación del sistema (4). En efecto si $(\xi_1,\ldots,\xi_n,\xi_{n+1})$ es una solución arbitraria del sistema (4), entonces

(6) $\xi_{n+1}\leqslant 0$

Ya que para $\xi_{n+1}>0$ el vector $\left(\xi_1\,\xi_{n+1}^{-1},\ldots,\xi_n\,\xi_{n+1}^{-1},1\right)$ sería una solución del sistema (4) que parte de (1), lo que contradice la hipótesis de la incompatibilidad de este sistema.

(1) Como la incompatibilidad (5) es una implicación del sistema (4), según el TEOREMA de Minkowski, el vector $(0,\ldots,0,1)$ puede ser representado bajo la forma de una combinación no negativa de vectores

$(a_{11}, \ \ldots, a_{1n}, -\gamma_1)$,

$(a_{m1}, \ \ldots, a_{m\ n}, -\gamma_m)$,

Dicho de otra manera existen números reales $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\gamma}_m$ tales que

$\boldsymbol{\lambda}_1 a_{11} + \ldots + \boldsymbol{\lambda}_m a_{m1} = 0$,

$\ldots \ldots \ldots \ldots \ldots$ $(\boldsymbol{\lambda}_1 \geqslant 0, \ \ldots, \boldsymbol{\lambda}_m \geqslant 0)$

$\lambda_1 a_{1n} + \ldots + \lambda_m a_{mn} = 0$,

$\lambda_1 \ (-\gamma_1) + \ldots + \lambda_m \ (-\gamma_m) = 1$.

Debido a (3) se deduce que

$\lambda_1 a_1 + \ldots + \lambda_m a_m = \mathbf{0}$,

$(\boldsymbol{\lambda}_1 \geqslant 0, \ \ldots, \boldsymbol{\lambda}_m \geqslant 0)$,

$\lambda_1 \gamma_1 + \ldots + \lambda_m \boldsymbol{\gamma}_m < 0$,

Es decir las condiciones (2) se cumplen.

Supóngase ahora que existen números reales $\lambda_1, \ \ldots, \lambda_m$ qu cumplen las condiciones (2) y demostremos que el sistema (1) es incompatible. Se considera la desigualdad

(7) $(\lambda_1 a_1 + \ldots + \lambda_m a_m)\, \mathbf{x} \leqslant \lambda_1 \gamma_1 + \ldots + \lambda_m \gamma_m$,

Que constituye una combinación lineal no negativa de desigualdades del sistema (1). Según la proposición 1.1. esta desigualdad es una implicación del sistema (1). Debido a (2), la desigualdad (7) puede ser escrito bajo la forma

$\mathbf{0}.\mathbf{x} < 0$.

Esta desigualdad no tiene soluciones y es una implicación del sistema (1), también el sistema (1) es incompatible. □

Sea $(a_{i1}, \ldots, a_{in})$ para $i = 1, \ \ldots, m$,

$$A = \begin{bmatrix} a_{11} \ldots a_{1n} \\ \ldots \ldots \\ a_{m1} \ldots a_{1m} \end{bmatrix}, \qquad {}^{t}A = \begin{bmatrix} a_{11} \ldots a_{m1} \\ \ldots \ldots \\ a_{1n} \ldots a_{mn} \end{bmatrix}.$$

TEOREMA 1.9. La desigualdad

(2) $\mathbf{bx} \leqslant 0$

Es una implicación de la desigualdad

(1) $\mathbf{Ax} \leqslant 0$

Si y sólo si el sistema

(3) ${}^{t}A\mathbf{y} = \mathbf{b}, \quad \mathbf{y} \geqslant 0,$

Es compatible.

El TEOREMA 1.9. Se deriva directamente de la proposición 1.1 y del TEOREMA 1.8

TEOREMA 1.10 *un sistema*

$\mathrm{A}\mathbf{x} + \mathbf{b} = \mathbf{0}, \quad \mathbf{x} \geqslant 0$
$(donde \ \mathbf{b} \ es\ una\ columna)$ *es compatible si y sólo si para todo*

$\mathbf{y}\ {}^{t}A\mathbf{y} \geqslant 0 \ \rightarrow {}^{t}\mathbf{by} \leqslant 0$

Al reemplazar en el TEOREMA 1.9 A , ${}^{t}A$, $\mathbf{b}$, ${}^{t}\mathbf{b}$, $\mathbf{x}$, $\mathbf{y}$ respectivamente para
$-{}^{t}A, -A$, ${}^{t}\mathbf{b}, \mathbf{b}$, $\mathbf{y}$, $\mathbf{x}$ esto demostrará que el TEOREMA 1.10 es únicamente una expresión del TEOREMA 1.9.

Soluciones no negativas de un sistema de ecuaciones lineales y de un sistema de inecuaciones lineales. El sistema de ecuaciones lineales

(1*) $\mathrm{a}_{i1}x_1 + \ldots + \mathrm{a}_{in}x_n + \beta_i = 0 \ (i = 1, \ \ldots, m),$

Puede ser escrito bajo la forma matricial

$$\mathrm{A}\mathbf{x} + \mathbf{b} = \mathbf{0},$$

Donde $\mathrm{A} = \|\mathrm{a}_{i\mathcal{R}}\|$es una matriz $m \times n$ y $\mathbf{b} = \begin{bmatrix} \beta_1 \\ . \\ . \\ . \\ \beta_m \end{bmatrix}$.

En el estudio de problemas de programación lineal estamos obligados a buscar las condiciones para las cuales el sistema (1*) admite al menos un solución no negativa. Esta búsqueda conduce a estudiar la compatibilidad del sistema

(1) $\mathrm{A}\mathbf{x} + \mathbf{b} = \mathbf{0}, \quad \mathbf{x} \geqslant \mathbf{0}.$

TEOREMA 1.11. El sistema (1) es compatible si y sólo si es incompatible el sistema

(2) ${}^{t}A\,\mathbf{y} \geqslant \mathbf{0}, \quad {}^{t}\mathbf{b}\,\mathbf{y} > 0.$

Demostración. Según el TEOREMA 1.10, el sistema (1), es compatible si y sólo si
(3) ${}^{t}\forall\,\mathbf{y}\ ({}^{t}A\,\mathbf{y} \geqslant \mathbf{0} \longrightarrow {}^{t}\mathbf{b}\,\mathbf{y} \leqslant 0).$

Se ve fácilmente que

$$\forall \mathbf{y}\,({}^{t}A\,\mathbf{y} \geqslant \mathbf{0} \longrightarrow {}^{t}\mathbf{b}\,\mathbf{y} \leqslant 0) \leftrightarrow \forall \mathbf{y}(\neg\, {}^{t}A \geqslant \mathbf{0}) \vee ({}^{t}A\,\mathbf{y}),$$
$$\leftrightarrow \forall \mathbf{y} \neg\, ({}^{t}A(\mathbf{y}) \geqslant 0 \wedge {}^{t}\mathbf{b}\,\mathbf{y} > \mathbf{0}).$$

Entonces, el sistema (1) es compatible si y sólo si para cada $\mathbf{y}$
$\neg\,({}^{t}A\,\mathbf{y} \geqslant 0 \wedge {}^{t}\mathbf{b}\,\mathbf{y} > 0)$.

Por lo tanto el sistema (1) es compatible si y sólo si es incompatible el sistema (2). □

TEOREMA 1.12. *El sistema*

(1) $A\,\mathbf{x} + \mathbf{b} \leqslant 0, \qquad \mathbf{x} \geqslant 0,$

Es compatible si y sólo si es compatible el sistema

(2) ${}^{t}A\,\mathbf{y} \geqslant 0, \qquad {}^{t}\mathbf{b}\,\mathbf{y} > 0, \qquad \mathbf{y} \geqslant 0.$

Demostración. Sea A una matriz $m \times n$ y $\mathbf{z}$ =

$$= \begin{bmatrix} \mathcal{Z}_1 \\ . \\ . \\ . \\ \mathcal{Z}_m \end{bmatrix}.$$

Se ve fácilmente que el sistema (1) es compatible si y sólo si es compatible el sistema

(1) $A\,\mathbf{x} + \mathbf{z} + \mathbf{b} = \mathbf{0}, \qquad \mathbf{x} \geqslant 0, \qquad \mathbf{z} \geqslant \mathbf{0}.$

E que es una matriz $m \times m$ unidad , tenemos

$A\,\mathbf{x} + \mathbf{z} + \mathbf{b} = A\,\mathbf{x} + E\mathbf{z} + \mathbf{b} = [\boldsymbol{A} \mid E] \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} + \mathbf{b}.$

También el sistema (1) puede ser escrito bajo la forma

$[\boldsymbol{A} \mid E] \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} + \mathbf{b} = \mathbf{0}, \qquad \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} \geqslant \mathbf{0}.$

Según el TEOREMA 1.11, el sistema (1´) es compatible si y solo si el sistema

$$\begin{bmatrix} {}^{t}A \\ E \end{bmatrix} \mathbf{y} \geqslant \mathbf{0}, \qquad {}^{t}\mathbf{by} > 0,$$

Es incompatible es decir que es incompatible el sistema

$${}^{t}A \geqslant \mathbf{0}, \qquad \mathbf{y} \geqslant \mathbf{0}, \qquad {}^{t}\mathbf{by} > 0.$$

Por lo tanto el sistema (1) es incompatible si y solo si es incompatible el sistema (2). □

Ejercicios.

1. Demostrar que cualquier sistema de n desigualdades lineales homogéneas para n variables, admite las soluciones no nulas.
2. Demostrar que la desigualdad $A\,\mathbf{x} \leqslant 0$ admite soluciones no nulas, si y sólo si las soluciones no nulas comprueba la desigualdad ${}^{t}A\mathbf{y} \leqslant 0$.

3. Demostrar que cualquier poliedro convexo constituye un conjunto de todas las soluciones de una serie de sistema de desigualdades lineales.
4. Mostrar que un conjunto de todas las soluciones de un sistema compatible de desigualdades lineales puede ser asimilado por la suma de un poliedro convexo y de un cono convexo generado por un conjunto finito de vectores.

§ 2. Problemas estándar y canónicos De la programación lineal. Teorema de dualidad

Problemas estándar y canónicos. Más adelante, en todas partes A es una matriz $m \times n$ en el cuerpo de números reales $\mathcal{R}$:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{bmatrix},$$

$\mathbf{b}$ y $\mathbf{c}$ siendo respectivamente vectores columnas de dimensión m y n sobre $\mathcal{R}$:

$$\mathbf{b} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}, \qquad \mathbf{c} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} \text{ y } {}^t\mathbf{b} = [\beta_1, \dots, \beta_m],$$

$${}^t\mathbf{c} = [\gamma_1, \dots, \gamma_n],$$

La forma lineal $\gamma_1 y_1 + \dots + \gamma_n y_n$ se escribirá como un producto

De la linea ${}^t\mathbf{c}$ y de la columna $\mathbf{y} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$, es decir

$${}^t\mathbf{cy} = \gamma_1 y_1 + \dots + \gamma_n y_n.$$

La forma lineal $\beta_1 z_1 + \dots + \beta_m z_m$. Se escribirá como un producto de la linea

${}^t\mathbf{b}$ para la columna $z = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$;

$${}^t\mathbf{bz} = \beta_1 z_1 + \dots + \beta_m z_m.$$

Los principales problemas de programación lineal se aplican a los problemas estándar y canónicos de mínimo y de máximo

P r o b l e m a s e s t a n d a r d e m i n i m i z a c i ó n

S. *Buscar la solución del sistema*

$$a_{i1}\mathcal{Y}_1 + \ldots + a_{in}\mathcal{Y}_n + \beta_i \leqslant 0 \qquad (i = 1, \ldots, m);$$

(1) $\mathcal{Y}_1 \geqslant \mathbf{0}, \ldots, \mathcal{Y}_n \geqslant \mathbf{0},$

Minimizando la forma lineal $\gamma_1\mathcal{Y}_1 + \ldots + \gamma_n\mathcal{Y}_n$.

P r o b l e m a s e s t a n d a r d e m a x i m i z a c i ó n

S^*. *Buscar la solución del sistema*

$$a_{1\mathcal{R}}\mathcal{Z}_1 + \ldots + a_{m\mathcal{R}}\mathcal{Z}_m + \gamma_{\mathcal{R}} \geqslant \mathbf{0} \ ,$$

(2)

$$\mathcal{Z}_1 \geqslant \mathbf{0}, \ldots, \mathcal{Z}_m \geqslant \mathbf{0},$$

Maximizando la forma lineal $\beta_1\mathcal{Z}_1 + \ldots + \beta_m\mathcal{Z}_m$.

Las condiciones (1) y (2) se llaman limitaciones lineales de los problemas S y S^*. Los problemas S y S^* son llamados *duales el uno del otro*.

Bajo la forma matricial esos problemas se enuncian de la manera siguiente:

S. *Buscar la solución del sistema*

(1) $\mathbf{Ay} + \mathbf{b} \leqslant 0, \qquad \boldsymbol{y} \geqslant \mathbf{0},$

Que minimiza la forma lineal ${}^t\mathbf{cy}$.

S. Buscar la solución del sistema*

$(\mathbf{2})$ ${}^t\mathbf{Az} + \mathbf{c} \geqslant \mathbf{0}, \qquad \mathbf{z} \geqslant \mathbf{0},$

Que maximiza la forma lineal ${}^t\mathbf{bz}$.

P r o b l e m a s c a n o n i c o d e m i n i m i z a c i ó n

C. *Buscar la solución del sistema*

(I) $a_{i1}\mathcal{Y}_1 + \ldots + a_{in}\mathcal{Y}_n + \beta_i = 0 \qquad (i = 1, \ldots, m),$

$$\mathcal{Y}_1 \geqslant \mathbf{0}, \ldots, \mathcal{Y}_n \geqslant \mathbf{0},$$

Que minimiza la forma lineal $\gamma_1\mathcal{Y}_1 + \ldots + \gamma_n\mathcal{Y}_n$.

P r o b l e m a d u a l d e l p r o b l e m a C

C*. *Buscar la solución del sistema*

$$(\text{II})\ a_{1\mathcal{R}}\mathcal{Z}_1+\ .\ .\ .+a_{m\mathcal{R}}\mathcal{Z}_m\ +\gamma_{\mathcal{R}}\geqslant \mathbf{0} \qquad (\ k=i,\ .\ .\ .,n),$$

Que Maximiza la forma lineal $\beta_1\,\mathcal{Z}_1+\ .\ .\ .+\beta_m\,\mathcal{Z}_m$.

Las condiciones (I) y(II) se llaman *condiciones de linealidad de problemas* C y C * *respectivamente los problemas* C y C**Son llamados duales el uno del otro.*

Estos problemas están constituidos bajo la forma matricial de la siguiente manera:

C. *Buscar la solución de sistema*

$$(\text{I})\quad \mathbf{Ay}+\mathbf{b}=\mathbf{0}, \qquad \mathbf{y}\geqslant\mathbf{0},$$

Que minimiza la forma lineal ${}^{t}\,\mathbf{cy}$

C * *buscar la solución de la desigualdad*

$$(\text{II})\quad {}^{t}\,\mathbf{Az}+\mathbf{c}\ \geqslant\mathbf{0},$$

Que maximiza la forma lineal ${}^{t}\,\mathbf{bz}$.

Vectores posibles y óptimos. Un problema de programación lineal es llamado *posible,* si existe un vector que cumple las condiciones de linealidad del problema. Si un tal vector existe, *es llamado vector posible del problema.*

Un vector posible se llama solución del problema o vector optimo del problema si se minimiza (en los problemas S y C) O maximiza (en los problemas S* y C*) la forma lineal del problema. El valor de este mínimo y de ese máximo es llamado *valor del problema de programación lineal.*

Designamos para $x_{1,\ .\ .\ .,}\ x_n$ los primeros miembros de la desigualdad del sistema (II)

Dicho de otra manera plantéese

(2) $x_{\mathcal{R}}=a_{1\mathcal{R}}\,\mathcal{Z}_1+\ .\ .\ .+a_{m\mathcal{R}}\,\mathcal{Z}_m+\gamma_{\mathcal{R}} \qquad (k=1,\ \ldots,n).$

PROPOSICIÓN 2.1 *Si el vector* $\begin{bmatrix}\mathcal{Y}_1\\ .\\ .\\ .\\ \mathcal{Y}_n\end{bmatrix}$ *, verifica las desigualdades*

(1´) $\mathrm{a}_{i1}\mathcal{Y}_1+\ .\ .\ .+\mathrm{a}_{in}\mathcal{Y}_n+\beta_i\leqslant 0 \qquad (\ i=1,\ .\ .\ .,m),$

entonces,

$$x_1\mathcal{Y}_1+\ .\ .\ .+x_n\mathcal{Y}_n\leqslant\ {}^{t}\,\mathbf{cy}-\ {}^{t}\,\mathbf{bz}.$$

D e m o s t r a c i ó n. Debido a (3),

$$x_1y_1+\ldots+x_ny_n=(a_{11}z_1+\ldots+a_{m1}z_m+\gamma_n)y_1+\ldots$$

$$\ldots+(a_{1n}z_1+\ldots+a_{mn}z_m+\gamma_n)y_n=$$
$$=(a_{11}y_1+\ldots+a_{1n}y_n)z_1+\ldots+(a_{m1}y_1+\ldots$$

$$\ldots+a_{mn}y_n)z_m+{}^t\mathbf{cy}.$$

Por lo tanto, en virtud de (1´),

$$x_1y_1+\ldots+x_ny_n\leqslant-(\beta_1z_1+\ldots+\beta_mz_m)+$$

$$+{}^t\mathbf{cy}={}^t\mathbf{cy}-+{}^t\mathbf{bz}.\quad\square$$

COROLARIO 2.2. Si $\mathbf{y}$ es un vector posible del problema estándar mínimo y $\boldsymbol{z}$
Un vector posible del problema dual, entonces

$$0\leqslant x_1y_1+\ldots+x_ny_n\leqslant{}^t\mathbf{cy}-{}^t\mathbf{bz}.$$

PROPOSICIÓN 2.3 *Si el vector* $\begin{bmatrix}y_1\\.\\.\\.\\y_n\end{bmatrix}$ *, verifica el sistema de ecuaciones*

$$(\mathrm{I}')\ \mathrm{a}_{i1}y_1+\ldots+\mathrm{a}_{in}y_n+\beta_i\leqslant0\qquad(i=1,\ \ldots,m),$$

entonces,

$$x_1y_1+\ldots+x_ny_n={}^t\mathbf{cy}-{}^t\mathbf{bz}.$$

Esta proposición se demuestra de manera similar a la proposición (2.1).

COROLARIO 2.4. *Si* $\mathbf{y}$ *es un vector posible del problema canónico mínimo y* $\boldsymbol{z}$ *un vector del problema dual, entonces*

$$0\leqslant x_1y_1+\ldots+x_ny_n\leqslant{}^t\mathbf{cy}-{}^t\mathbf{bz}.$$

PROPOSICIÓN 2.5. *si* $\mathbf{y}$ *es un vector posible del problema mínimo (S ó* C*) y* $\boldsymbol{z}$
Un vector posible del problema dual (S* ó C*), entonces ${}^t\mathbf{cy}-{}^t\mathbf{bz}\geqslant0$.

La proposición 2.5 se deriva directamente de los corolarios 2.2 y 2.4.

PROPROSICIÓN 2.6 (CRITERIO DE OTIMIZACIÓN DE VECTORES) si $\mathbf{y}$
Es un vector posible del problema mínimo, $\boldsymbol{z}$ *es un vector posible del problema dual y* ${}^t\mathbf{cy}-{}^t\mathbf{bz}$ *, entonces* $\mathbf{y}$ y $\boldsymbol{z}$ *son vectores óptimos de los problemas correspondientes*.

Demostración. Sea $\mathbf{y}'$ un vector posible del problema del mínimo. Según la proposición 2.5,

${}^t\mathbf{cy} \geqslant {}^t\mathbf{bz}$. Además , por hipótesis, ${}^t\mathbf{bz} = {}^t\mathbf{cy}$, por tanto ${}^t\mathbf{cy}' \geqslant {}^t\mathbf{cy}$ cual quiera que sea el vector posible $\mathbf{y}'$ del problema mínimo. Por lo tanto, $\mathbf{y}$ es el vector óptimo del problema mínimo.

De manera similar demuéstrese que $\mathbf{z}$ es el vector óptimo del problema máximo. □

TEOREMA de dualidad de los problemas estándar. En teoría de programación lineal los TEOREMAs de dualidad 2.7 y 2.8 son esenciales.

TEOREMA 2.7. *Si dos problemas estándar duales el uno del otro (*S y S*), son posibles, eso dos problemas tienen soluciones y los valores de esos problemas son idénticos. Si al menos uno de los problemas es imposible, entonces ninguno de los problemas tiene solución.*

D e m o s t r a c i ó n. Supóngase que los dos problemas son imposibles. Entonces, el sistema

(1) $\boldsymbol{A}\mathbf{y} + \mathbf{b} \leqslant 0, \qquad \mathbf{y} \geqslant 0,$

(2) ${}^t\mathbf{cy}' + \mathbf{c} \geqslant 0, \qquad \mathbf{z} \geqslant 0$

Es compatible.

La primera parte del TEOREMA será demostrado si demostramos la existencia de las Soluciones $\mathbf{y}$ y $\boldsymbol{z}$ respectivamente para el sistema (1) y (2)que se comprueban

(3) ${}^t\mathbf{cy} - {}^t\mathbf{bz} \leqslant 0.$

En efecto, en este caso según la proposición 2.5 los vectores posibles $\mathbf{y}\ y\ \mathbf{z}$ comprueban la desigualdad ${}^t\mathbf{cy} - {}^t\mathbf{bz}$. Por lo tanto si $\mathbf{y}\ y\ \mathbf{z}$ comprueban igualmente (3) tenemos entonces ${}^t\mathbf{cy} - {}^t\mathbf{bz}$ Como resultado, en virtud de criterio de optimización , los vectores $\mathbf{y}\ y\ \mathbf{z}$ Son los vectores óptimos de los problemas correspondientes (S y S)* y los valores de dos Problemas coincidirán, entonces solo basta con demostrar la compatibilidad del sistema

$$(4)\begin{cases} \mathbf{Ay} + \mathbf{b} \leqslant \mathbf{0}, & \mathbf{y} \geqslant \mathbf{0}, \\ -{}^t\mathbf{Az} - \mathbf{c} \leqslant \mathbf{0}, & \boldsymbol{z} \geqslant \mathbf{0}, \\ {}^t\mathbf{cy} - {}^t\mathbf{bz} \leqslant 0. \end{cases}$$

Escríbase este sistema bajo la forma matricial:

$$(4)\quad \begin{bmatrix} A & 0 \\ 0 & -{}^t\mathbf{A} \\ {}^t\mathbf{c} & -{}^t\mathbf{b} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ -\mathbf{c} \\ 0 \end{bmatrix} \leqslant \mathbf{0}, \qquad \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} \geqslant \mathbf{0}.$$

Según el TEOREMA 2.6 el sistema (4) es compatible si y sólo si es incompatible el sistema

$$(5)\quad \begin{bmatrix} {}^t\boldsymbol{A} & 0 & \mathbf{c} \\ 0 & -\boldsymbol{A} & -\mathbf{b} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \\ -\lambda \end{bmatrix} \geqslant \mathbf{0}, \qquad {}^t\mathbf{bu} - {}^t\mathbf{cv} > 0, \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \\ -\lambda \end{bmatrix} \geqslant \mathbf{0},$$

Este sistema se puede escribir bajo la forma

$$\mathbf{Av}+\mathbf{b}\lambda \leqslant \mathbf{0},$$
$$(5)\quad -{}^{t}\mathbf{Au}-\mathbf{c}\lambda \leqslant \mathbf{0}\ ,\qquad \mathbf{u}\geqslant \mathbf{0}\qquad ,\qquad \mathbf{v}\geqslant \mathbf{0}\quad ,\qquad \boldsymbol{\lambda}\geqslant \mathbf{0}$$
$${}^{t}\mathbf{cv}-{}^{t}\mathbf{bu}<0.$$

Muéstrese que el sistema (5) es incompatible. Admítase que existen los vectores $\mathbf{u}$ y $\mathbf{v}$ y un número real λ que comprueba las desigualdades (5).Entonces para $\lambda<0$ se tiene:

$$\mathbf{A}\left(\mathbf{v}\lambda^{-1}\right)+\mathbf{b}\leqslant \mathbf{0},\qquad \mathbf{v}\lambda^{-1}\geqslant \mathbf{0},$$
$$(5')\quad -{}^{t}\mathbf{A}\left(\mathbf{u}\lambda^{-1}\right)-\mathbf{c}\leqslant \mathbf{0},\qquad \mathbf{u}\lambda^{-1}\geqslant \mathbf{0},$$
$${}^{t}\mathbf{c}\left(\mathbf{v}\lambda^{-1}\right)-{}^{t}\mathbf{b}\left(\mathbf{u}\lambda^{-1}\right)<0.$$

Las primeras cuatros desigualdades muestran que los vectores $\mathbf{v}\lambda^{-1}$ y $\mathbf{u}\,\lambda^{-1}$ Satisfacen respectivamente las condiciones (1) y (2), es decir tienen vectores posibles de los problemas correspondientes. Por lo tanto según la proposición 2.5,

$${}^{t}\mathbf{c}\,(\mathbf{v}\lambda^{-1})-\ {}^{t}\mathbf{b}\,(\mathbf{u}\,\lambda^{-1})\geqslant \mathbf{0},$$

lo que contradice la última desigualdad (5´).

Pero si $\lambda=0$, el sistema (5) es incompatible. En efecto, por hipótesis, es compatible el sistema (1), (2), es decir el sistema

$$(6)\begin{bmatrix}\mathbf{A} & 0\\ 0 & -{}^{t}\mathbf{A}\end{bmatrix}\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix}+\begin{bmatrix}\mathbf{b}\\ -\mathbf{c}\end{bmatrix}\leqslant \mathbf{0},\quad \begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix}\geqslant \mathbf{0}.$$

Según el TEOREMA 2.6, de la compatibilidad del sistema (6) se deduce la incompatibilidad del sistema

$$\begin{bmatrix}{}^{t}\mathbf{A} & 0\\ 0 & -\mathbf{A}\end{bmatrix}\begin{bmatrix}\mathbf{u}\\ \boldsymbol{z}\end{bmatrix}\geqslant \mathbf{0},\qquad {}^{t}\mathbf{bu}-\ {}^{t}\mathbf{cv}>\mathbf{0},\qquad \begin{bmatrix}\mathbf{u}\\ \boldsymbol{z}\end{bmatrix}\geqslant \mathbf{0},$$

es decir es incompatible el sistema

$$\mathbf{Av}\leqslant \mathbf{0},$$
$$-\ {}^{t}\mathbf{Au}\ \leqslant \mathbf{0},\qquad \mathbf{u}\geqslant \mathbf{0},\qquad \mathbf{v}\geqslant \mathbf{0},$$
$${}^{t}\mathbf{cv}-\ {}^{t}\mathbf{bu}<\mathbf{0}.$$

Así, el sistema (5) es incompatible, y como resultado el sistema (4) es compatible.

Supóngase ahora que es posible únicamente uno de los dos problemas duales, uno del otro, por ejemplo, el problema S, mientras que él S^* no lo es. Demuéstrese entonces que el problema S no tiene soluciones. La posibilidad del primer problema significa que existe una solución $\boldsymbol{y}'$ del sistema (1), es decir

$$(1')\quad \boldsymbol{A}\,\mathbf{y}'+\mathbf{b}\ \leqslant\ \mathbf{0},\qquad \mathbf{y}'\geqslant\ \mathbf{0},$$

La imposibilidad del problema S^*, es decir al incompatibilidad del sistema

$$(2)\quad -{}^{t}\mathbf{Az}-\mathbf{c}\leqslant \mathbf{0},\qquad \mathbf{z}\geqslant\ \mathbf{0},$$

implica, según el TEOREMA 1.12, la compatibilidad del sistema

(2*) $\mathbf{Ax} \leqslant \mathbf{0}$, $\quad {}^{t}\mathbf{cx} \leqslant \mathbf{0}$, $\quad \mathbf{x} \leqslant \mathbf{0}$.

Por consiguiente, existe un vector $\mathbf{x}'$ tal que

(2´) $\mathbf{Ax}' \leqslant \mathbf{0}$, $\quad {}^{t}\mathbf{cx}' < \mathbf{0}$, $\quad \mathbf{x}' \geqslant \mathbf{0}$

Sobre la base de (1´) y (2´) concluimos que para todo n natural se comprueban las desigualdades

(7) $\mathbf{A}(\mathbf{y}' + \boldsymbol{n}\mathbf{x}') + \mathbf{b} \leqslant \mathbf{0}$, $\quad \mathbf{y}' + \boldsymbol{n}\mathbf{x}'' \geqslant \mathbf{0}$

Por tanto, para cualquier n natural el vector $\mathbf{y}' + \boldsymbol{n}\mathbf{x}'$ es un vector posible del primer problema. De todos modos, la forma lineal ${}^{t}\mathbf{cy}$ no tiene mínimo. De hecho,

${}^{t}\mathbf{c}(\mathbf{y}' + \boldsymbol{n}\mathbf{x}') = {}^{t}\mathbf{cy}' + n\ ({}^{t}\mathbf{cx}')' +$

en la suma del segundo miembro el primer término es un cierto número real, en cuanto al segundo término, debido al ${}^{t}\mathbf{cx}' < \mathbf{0}$ **,** puede ser devuelto para un m suficientemente grande, inferior a todos los números determinados**.** Entonces La forma lineal ${}^{t}\mathbf{cy}$ no tiene mínimo, en otras palabras, el primer problema no tiene soluciones. □

TEOREMA de dualidad para los problemas canónicos. Examínese los problemas canónicos C y C *:

C. Buscar la solución del sistema $\boldsymbol{A}\mathbf{y} + \boldsymbol{b} = \mathbf{0}, \mathbf{y} \geqslant \mathbf{0}$ minimizando la forma lineal ${}^{t}\mathbf{cy}$ **.**

C*. Buscar la solución de desigualdad ${}^{t}\mathbf{Az} + \mathbf{c} \geqslant \mathbf{0}$, maximizando la forma lineal ${}^{t}\mathbf{bz}$.

El problema C es equivalente al problema estándar siguiente:

S_1. *Buscar la solución del sistema*

$$\begin{bmatrix} -\boldsymbol{A} \\ \boldsymbol{A} \end{bmatrix}\mathbf{y} + \begin{bmatrix} -\mathbf{b} \\ \mathbf{b} \end{bmatrix} \leqslant \mathbf{0}, \quad \mathbf{y} \geqslant \mathbf{0},$$

minimizando la forma lineal ${}^{t}\mathbf{cy}$.

El problema dual es el problema siguiente:

S_1*. *Buscar la solución del sistema*

$$[-{}^{t}\mathbf{A}|{}^{t}\mathbf{A}|]\begin{bmatrix}\mathbf{z}' \\ \mathbf{z}''\end{bmatrix} + \mathbf{c} \geqslant \mathbf{0}, \qquad \begin{bmatrix}\mathbf{z}' \\ \mathbf{z}''\end{bmatrix} \geqslant \mathbf{0}$$

donde, $\mathbf{z}' = \begin{bmatrix} \boldsymbol{z_1} \\ \cdot \\ \cdot \\ \cdot \\ \boldsymbol{z_m} \end{bmatrix}$, $\mathbf{z}'' = \begin{bmatrix} \boldsymbol{z_{m+1}} \\ \cdot \\ \cdot \\ \cdot \\ \boldsymbol{z_{2m}} \end{bmatrix}$, maximiza la forma lineal

$$[-{}^{t}\mathbf{b}|{}^{t}\mathbf{b}|]\begin{bmatrix}\mathbf{z}' \\ \mathbf{z}''\end{bmatrix}$$

Se ve fácilmente que el problema S_1* es equivalente al problema C_1*. En efecto,

$$[-{}^{t}\mathbf{A}|{}^{t}\mathbf{A}|]\begin{bmatrix}\mathbf{z}' \\ \mathbf{z}''\end{bmatrix} = {}^{t}\mathbf{A}(\mathbf{z}'' - \mathbf{z}'), \quad [-{}^{t}\mathbf{b}|{}^{t}\mathbf{b}|]\begin{bmatrix}\mathbf{z}' \\ \mathbf{z}''\end{bmatrix} = {}^{t}\mathbf{b}(\mathbf{z}'' - \mathbf{z}').$$

Todo vector de dimensión m puede ser representado bajo la forma de una diferencia de dos vectores no negativos de dimensión m .como resultado, si colocamos $\mathbf{z} = \mathbf{z}'' - \mathbf{z}'$**,** en el trayecto del conjunto de todo esos vectores de dimensión m de $\boldsymbol{R}^m$ cuando $\mathbf{z}''$ y $\mathbf{z}'$ recorren el conjunto de todos los vectores no negativos$\boldsymbol{R}^m$.

Por lo tanto, el problema S_1*. Es equivalente al siguiente problema (que coincide con el problema C*).buscar la solución de la desigualdad $\mathbf{Az} + \mathbf{c} \geqslant \mathbf{0}$ maximizando la forma lineal ${}^{t}\mathbf{bz}$.

Los problemas estándar $S_1 \; y \; s_1^*$ son duales el uno del otro y por ellos se verifica el TEOREMA de dualidad. Los problemas C y C^* son respectivamente equivalentes a los problemas $S_1 \; y \; s_1^*$ .así que el TEOREMA de dualidad se aplica también a los problemas de dualidad C y C^* , es decir que tenemos al TEOREMA siguiente.

TEOREMA 2.8. Si dos problemas canónicos duales el uno del otro $(C \; Y \; C^*)$ son posibles, entonces los dos problemas admiten soluciones y los valores de estos problemas coinciden. Si al menos uno de estos problemas es imposible, entonces ninguno de los problemas admiten soluciones.

TEOREMA de equilibrio: Recuérdese que se convino designar para $x_1, \ldots, x_n$ los primeros miembros de desigualdades del sistema $(\mathbf{II})$,

$$\mathcal{X}_{\mathcal{R}} = a_{1\mathcal{R}}\mathcal{Z}_1 + \ldots + a_{mn}\mathcal{Z}_m \qquad (k = 1, \ldots, n)$$

TEOREMA 2.9 *Sean* $\boldsymbol{y} = \begin{bmatrix} \boldsymbol{\mathcal{Y}_1} \\ . \\ . \\ . \\ \boldsymbol{\mathcal{Y}_n} \end{bmatrix}$ *el vector posible del*

problema canónico mínimo y $z = \begin{bmatrix} \boldsymbol{\mathcal{Z}_1} \\ . \\ . \\ . \\ \boldsymbol{\mathcal{Z}_m} \end{bmatrix}$ *el vector posible del*

problema dual. Si

$$(*) \quad \mathcal{X}_1\mathcal{Y}_1 = 0, \ldots, \mathcal{X}_n\mathcal{Y}_n = 0,$$

entonces $\boldsymbol{y} \; y \; \boldsymbol{z}$ *son los vectores óptimos de los problemas correspondientes* $(C \; Y \; C^*)$.

Demostración. Supóngase que las condiciones$(*)$ se cumplen. Según el corolario 2.4, se tiene

(1) $0 \leqslant \mathcal{X}_1\mathcal{Y}_1 + \ldots + \mathcal{X}_n\mathcal{Y}_n = {}^{t}\mathbf{cy} - {}^{t}\mathbf{bz}$.

Sobre la base de (*) y (1) se concluye que ${}^{t}\mathbf{cy} - {}^{t}\mathbf{bz} = 0$. Según el criterio de optimalidad los vectores $\mathbf{y}$ y $\mathbf{z}$ son los vectores óptimos respectivamente de los problemas C Y C.* □

Observación: La condición (*) es igualmente necesaria para los vectores posibles $\mathbf{y}$ y $\mathbf{z}$ sean óptimos. En efecto, según el corolario 2.4, (1) se verifica. Si los vectores $\mathbf{y}$ y $\mathbf{z}$ son óptimos, entonces el TEOREMA 2.8,

(2) ${}^{t}\mathbf{cy} - {}^{t}\mathbf{bz}$.

De (1) y (2) se deduce

$= {}^{t}\mathbf{cy} - {}^{t}\mathbf{bz}$.

$0 \leqslant \mathcal{X}_1\mathcal{Y}_1 + \ldots + \mathcal{X}_n\mathcal{Y}_n = 0$.

Ya que $\mathbf{y}$ y $\mathbf{z}$ son los vectores posibles, se tiene $\mathcal{X}_1, \ldots, \mathcal{X}_n \geqslant 0$ y $\mathcal{Y}_1 \ldots, \mathcal{Y}_n \geqslant 0$. De allí se deducen las igualdades (*).

Ejercicios

1. Mostrar que si uno de los problemas duales el uno del otro de la programación lineal (canónicos o estándar) admite una solución, entonces el otro igualmente la tiene.
2. dar un ejemplo de problema estándar (canónico) como mínimo de dos variables, que al igual que su dual no sea posible.
3. Construir un ejemplo de problema estándar de mínimo que admite más de una solución óptima.

§ 3. Método simplex (método de Dantzig)

Método de simplex. Dantzig elaboró el método de simplex para los problemas de programación lineal. En el método simple de resolución simultánea de dos problemas canónicos duales el uno del otro expuesto más adelante se refiere a Hall [28].

Considérense los problemas duales el uno del otro.

C. *Buscar la solución del sistema*

$$\alpha_{11}\mathcal{Y}_1 + \ldots + \alpha_{1n}\mathcal{Y}_n + \beta_1 = 0,$$

(I) $\ldots\ldots\ldots\ldots\ldots\ldots \quad \mathcal{Y}_1 \geqslant 0, \ldots, \mathcal{Y}_n \geqslant 0,$

$$\alpha_{m1}\mathcal{Y}_1 + \cdots + \alpha_{mn}\mathcal{Y}_n + \beta_m = 0,$$

al maximizar la forma lineal v*:*

$$\gamma_1\mathcal{Y}_1 + \ldots + \gamma_n\mathcal{Y}_n = v.$$

$\mathbf{C}^*$. *Buscar la solución del sistema*

$$\boldsymbol{\alpha_{11}}\mathcal{Z}_1 + \ldots + \alpha_{m1}\mathcal{Z}_m + \boldsymbol{\gamma_1} \geqslant 0,$$

(II) $\ldots\ldots\ldots\ldots\ldots\ldots$

$$\boldsymbol{\alpha_{1n}}\mathcal{Z}_1 + \ldots + \alpha_{mn}\mathcal{Z}_m + \boldsymbol{\gamma_n} \geqslant 0,$$

al maximizar la forma lineal u*:*

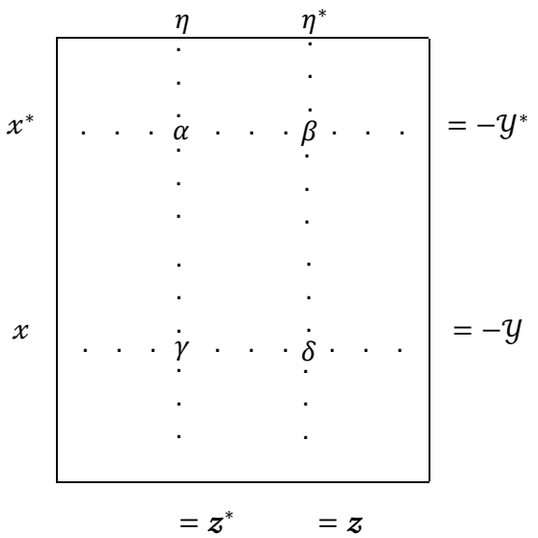
$$\beta_1\mathcal{Z}_1 + \ldots + \beta_m\mathcal{Z}_m = \mathrm{u}.$$

El método de simplex es el método que permite resolver los problemas simultáneamente canónicos duales C Y C^* el uno del otro.

sea $A = \begin{bmatrix} a_{11} \ldots a_{1n} \\ \cdots\cdots\cdots \\ a_{m1} \ldots a_{mn} \end{bmatrix}$. La matriz del sistema de ecuación $(\mathbf{I})$.

Se admite que más adelante del rango de la matriz A es m; esta hipótesis simplifica un poco la exposición esquemática del método de simplex. Podemos reducir el caso general a este caso estudiado.

Considérese la tabla



En esta tabla se presta a la interpretación simultánea de dos sistemas de ecuaciones lineales. Este representa el sistema lineal que corresponde a las filas:

(1)

$$\cdots a\boldsymbol{\eta}^* + \cdots + \boldsymbol{\beta\eta} + \cdots = -y^*,$$

$$\cdots \gamma\boldsymbol{\eta}^* + \cdots + \boldsymbol{\delta\eta} + \cdots = -y,$$

y que corresponde a las columnas:

(2)

$$\cdots a\boldsymbol{x}^* + \cdots + \boldsymbol{\gamma x} + \cdots = -\boldsymbol{z}^*$$

$$\cdots \beta x^* + \cdots + \delta x + \cdots = -, z.$$

La *transformación de la tabla con el elemento pivote* $\alpha(\alpha \neq 0)$, sustituye a la tabla de inicio que corresponde a la solución del sistema (1) en relación a $-\eta^*$ y a la solución del sistema (2) con relación a x^*.

Una vez resuelta la ecuación del sistema (1) que incluye al elemento pivote α en relación a $-\eta^*$, se deduce $\cdots + \alpha^{-1} y^* + \cdots + \alpha^{-1}\beta\eta + \cdots = -\eta^*$.

(1) Al llevar esta expresión de $-\eta^*$ en las otras ecuaciones del sistema (1), se obtiene:

$$\cdots + \alpha^{-1} y^* + \cdots + \alpha^{-1}\beta\eta + \cdots = -\eta^*,$$

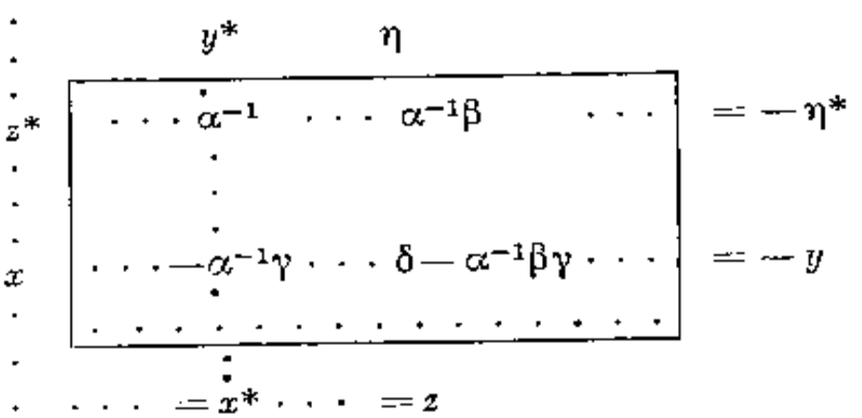
$$\cdots + \alpha^{-1}\gamma y^* + \cdots + (\delta - \alpha^{-1}\beta\gamma)\eta + \cdots = -y.$$

De manera análoga, al resolver el sistema (2) que corresponde a x^*, se deduce

(2)
$$\cdots \alpha^{-1} z^* + \cdots + (-\alpha^{-1}\gamma)\, x + \ldots = x,^*,$$

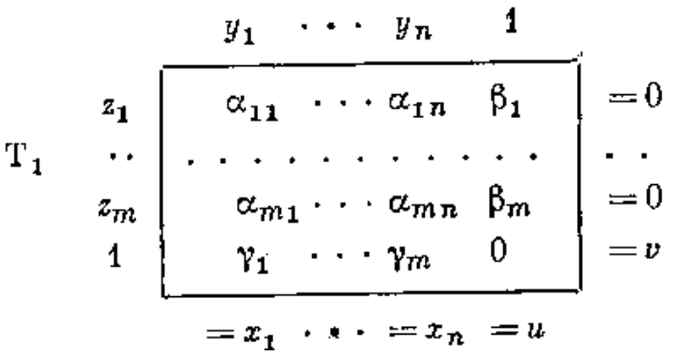
$$\cdots \alpha^{-1}\beta z^* + \cdots + (\delta - \alpha^{-1}\beta\gamma)\, x + \ldots = z.$$

Así, la transformación de la tabla con el elemento pivote α remplaza a la tabla de inicio por la siguiente tabla:



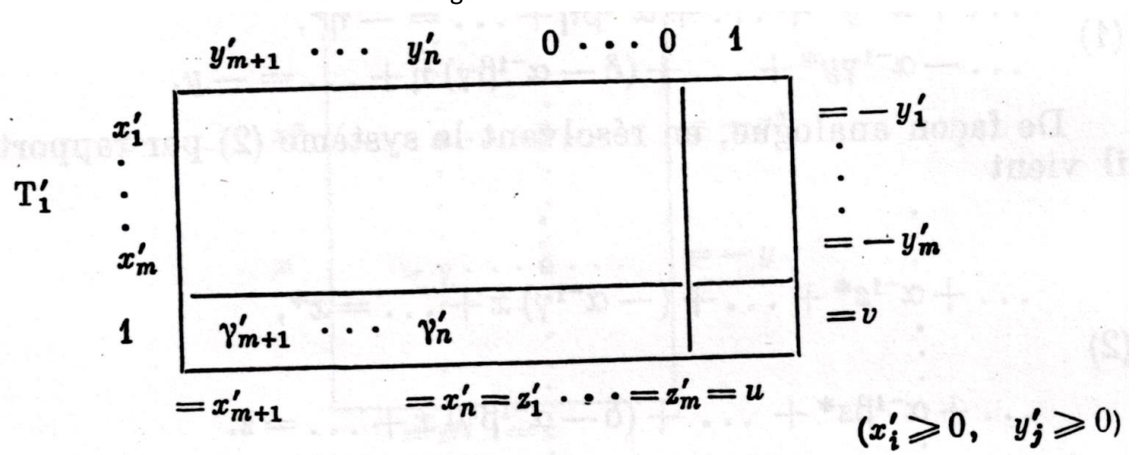
que corresponde a la solución del sistema (1) que sigue las filas con relación a $-\eta^*$ y del sistema (2) que sigue las columnas con relación a x^*.

Los dos problemas canónicos C y C^* duales el uno del otro encuentran su representación en la tabla



Búsquese simultáneamente las soluciones de los dos problemas. Despéjese en seguida las variables $z_1, \ldots, z_m$ que no están sometidas a restricciones. Es la primera etapa de la resolución. Esta se implementa por una sucesión de transformaciones con pivote partiendo de la tabla T_1.

Las operaciones se realizan hasta la aparición en la tabla de un elemento no nulo con una y debajo y el cero a la derecha sobre la fila. Finalmente se obtiene la tabla de la siguiente forma



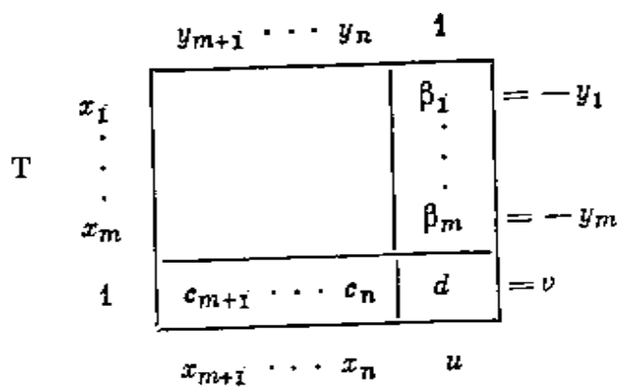
En este tabla las variables con primos representan en un orden diferente las variables que figuran en la tabla de inicio T_1, las filas y las columnas se cambiaron en relación a la posición de los ceros. Las m últimas columnas representan las ecuaciones que expresan las variables $z'_1, \ldots, z'_m$ en función de las variables $x'_1, \ldots, x'_m$. Estas ecuaciones deben extraerse:

$$z'_1 = d_{11}x'_1 + \ldots + d_{1m}x'_m,$$

(III) $\cdots\cdots\cdots\cdots\cdots$

$$z'_m = d_{m1}x'_1 + \ldots + d_{mm}x'_m.$$

Luego, se debe considerar únicamente las igualdades que unen las variables $z'_1, \ldots, z'_m$ que se expresan en la parte de la tabla T_1 que incluye las $n - m$ primeras columnas. Así, luego de la eliminación de las variables $z'_1, \ldots, z'_m$, resulta la tabla



La tabla T se denomina posible de acuerdo a las filas, si satisface las condiciones

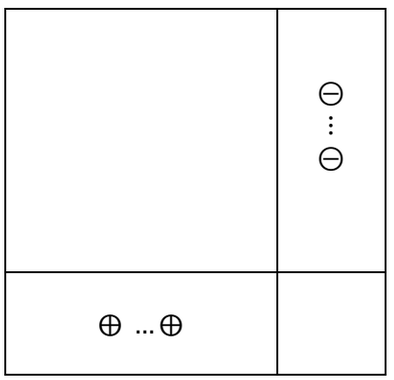
$$(1)\beta_1 \leqslant 0, \ldots \beta_m \leqslant 0.$$

Estas condiciones traducen que el vector $(-\beta_1, \ldots, \beta_m, 0, \ldots, 0)$ es el vector posible del problema C, es decir que verifica al sistema (I). Supóngase que La tabla T es posible de acuerdo a las filas, es decir que las condiciones (1) se cumplan, el objetivo de la etapa siguiente de la resolución del problema es buscar a través una serie de transformaciones con pivote en La tabla obtenida de T, los vectores posibles de dos problemas C y C^* que cumplen las condiciones.

$$(*)\ x_1y_1 = 0, \ldots, x_ny_n = 0 \qquad (x_i \geqslant 0, y_i \geqslant 0).$$

Según el TEOREMA de equilibrio, estos vectores serán los vectores óptimos de los problemas correspondientes.

Introdúzcanse las notaciones: $\oplus$ un número no negativo, $\ominus$ un número no positivo. Plantéese que se parte de la tabla T y que se está en la posibilidad de pasar la tabla de la forma



Entonces al proporcionar las variables libres $x_1, \ldots, x_m$ y $y_{m+1}, \ldots, y_n$ de los valores nulos se obtienen los vectores posibles de los problemas $(\mathrm{C}$ y $\mathrm{C}^*)$ que constituyen los vectores óptimos de estos problemas.

Véase la influencia de la trasformación con el elemento pivote sobre las columnas de términos $\boldsymbol{\alpha_{rs}}$ libres, y el valor de la forma linear $\boldsymbol{v}$ para minimizar:

$\boldsymbol{\alpha_{rs}} \ldots \boldsymbol{\beta_r} \quad \ldots \quad \boldsymbol{\alpha_{rs}^{-1}} \quad \ldots \boldsymbol{\alpha\alpha_{rs}^{-1}\beta},$

$\ldots\ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\boldsymbol{\alpha_{is}} \ldots \boldsymbol{\beta_i} \quad \ldots - \boldsymbol{\alpha_{rs}^{-1}}\alpha_{is} \ldots \boldsymbol{\beta_i} - \boldsymbol{\alpha_{rs}^{-1}\beta_r}\alpha_{is}$,

$\ldots\ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\boldsymbol{\gamma_s} \ldots \boldsymbol{\delta} \quad \ldots - \boldsymbol{\alpha_{rs}^{-1}}\gamma_s \ldots \boldsymbol{\delta} - \boldsymbol{\alpha_{rs}^{-1}\beta_r}\gamma_s.$

Supóngase que en la tabla (a la izquierda) los elementos de la columna de términos libres no son positivos, es decir

$(\mathbf{1})\ \beta_i \leqslant 0 \qquad (i = 1, \ldots, m).$

Se necesita que en el nuevo valor de la forma lineal v no sea superior a la anterior, es decir que $\boldsymbol{\delta} - \boldsymbol{\alpha_{rs}^{-1}\beta_r}\gamma_s \leqslant \boldsymbol{\delta}$.Esta desigualdad se verifica si se cumplen las condiciones

$(a) \qquad \boldsymbol{\alpha_{rs}} > \mathbf{0}, \qquad \gamma_s < \mathbf{0}.$

Con la satisfacción de estas condiciones el nuevo valor de la forma lineal v no es superior a la anterior, así mismo el nuevo valor de la forma v para $\beta_r < 0$ es estrictamente inferior a la anterior.

Además, es necesario que los nuevos elementos de la columna de los términos libres sean no positivos es decir que

$\boldsymbol{\beta_i - \alpha_{rs}^{-1}\beta_r\alpha_{is} \leqslant 0}$.

Con la satisfacción de las condiciones (α) y para $\boldsymbol{\alpha_{is} \leqslant 0}$ esta desigualdad se verifica. En cambio si $\boldsymbol{\alpha_{is} > 0}$ la desigualdad se puede escribir de la siguiente forma

$(\beta)\ \frac{\beta_r}{\alpha_{rs}} \geqslant \frac{\beta_i}{\alpha_{is}}$ para cualesquieras $\boldsymbol{\alpha_{is} > 0} \qquad (i \neq r)$.

Se obtiene así la *regla* siguiente *de la selección del elemento pivote* de la transformación de la tabla posible que corresponde a las filas.

Sea una tabla posible que corresponde a las filas. *En lugar del elemento pivote* (*de la transformación*) *se tiene que seleccionar el elemento* a_{rs} *si se satisfacen las condiciones:*

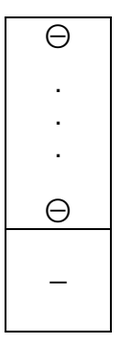
$(a)\boldsymbol{\gamma_s < 0},\ \alpha_{rs} > 0;$

$(\beta)\ \frac{\beta_r}{a_{rs}} \geqslant \frac{\beta_i}{\alpha_{is}}$ con $\alpha_{is} > 0\ (i \neq r)$.

De acuerdo a esta regla la elección del elemento pivote garantiza la posibilidad de una nueva tabla siguiendo las filas y para $\beta_r < 0$ proporciona un nuevo valor de la forma lineal v (para minimizar) estrictamente de la inferior a la anterior.

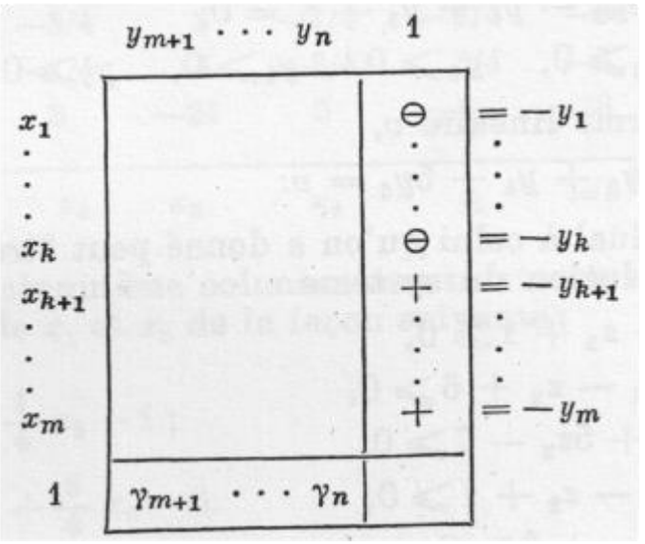
Partiendo de la tabla posible se efectúa por filas la sucesión de las trasformaciones con pivote de acuerdo a la regla de elección del elemento pivote. La operación se concluye cuando en la última fila de la tabla no tenga más elementos negativos; eso significa que la tabla es así mismo posible por filas que por columnas, es decir que se encontraron las soluciones de los dos problemas C y C^* (se obtuvieron los vectores óptimos).

El proceso también le pone fin al caso del que se plantea en la tabla con una columna negativa (que no es la última) de la forma



y ,como resultado, la regla de elección del elemento pivote es inaplicable. Esto significa que el problema C^* es imposible, puesto que no se satisfacen las condiciones $x_s \geqslant 0$.

La tabla T resulta imposible así mismo para filas como para columnas. En ese caso se busca la solución posible del problema C o se estable la imposibilidad del problema C^* que procede de la siguiente forma. Las filas de la tabla T se permutan de manera que todas las filas posibles se encuentren arriba de la tabla:



Las $k+1$ primeras filas de esta tabla se considerarán como una tabla posible para filas, y se procurará minimizar $(-\mathcal{Y}_{\mathcal{R}+1})$. si en el trascurso del camino resulta un valor no positivo de $(-\mathcal{Y}_{\mathcal{R}+1})$, se obtendrá entonces $k+1$ posibles filas o mayor. Se prosigue con el proceso de manera análoga buscando la representación de un gran número de filas en forma posible. Si una fila positiva aparece en la tabla, es decir una fila (imposible) de la siguiente forma

$\oplus \cdot \cdot \cdot \oplus$	$+$

↘

esto significará que el problema C es imposible, puesto que no puede cumplir la condición $-\mathcal{Y}j \leqslant 0$.

Si por el contrario, resulta que el valor mínimo de $(-\mathcal{Y}_{\mathcal{R}+1})$es positivo, se tiene la tabla la siguiente forma

		$\ominus$ $\cdot$ $\cdot$ $\cdot$ $\ominus$
$-$		$+$

$= \mathcal{Y}_{\mathcal{R}+\circledcirc 1}$

En este caso a modo de elemento pivote se eligió el elemento señalado por una flecha. Se comprueba fácilmente que esta elección provee $k+1$ filas posibles o más. Se obtuvo así el procedimiento que permite encontrar la solución posible del problema en todos los casos posibles.

Problema. Buscar la solución del sistema.

$$5y_1 - 4y_2 + 13y_3 - 2y_4 + y_5 - 20 = 0,$$

(I) $$y_1 - y_2 + 5y_3 - y_4 + y_5 - 8 = 0,$$

$$y_1 \geqslant 0, \quad y_2 \geqslant 0, \quad y_3 \geqslant 0, \quad y_4 \geqslant 0, \quad y_5 \geqslant 0,$$

que minimiza la forma lineal v,

$$y_1 + 6y_2 - 7y_3 + y_4 + 5y_1 = v.$$

El problema dual que se ha dado puede ser formulado de esta manera: buscar la solución del sistema

$$x_1 = 5z_1 + z_2 + 1 \geqslant 0,$$

$$x_2 = 4z_1 - z_2 + 6 \geqslant 0,$$

(II) $$x_3 = 13z_1 + 5z_2 - 7 \geqslant 0,$$

$$x_4 = -2z_2 - z_2 + 1 \geqslant 0,$$

$$x_5 = z_1 + z_2 + 5 \geqslant 0,$$

que maximiza la forma lineal u,

$$-20z_1 - 8z_2 = \boldsymbol{u}.$$

Estos dos problemas se representan por la siguiente tabla:

	y_1	y_2	y_3	y_4	y_5	1	
z_1	5	−4	13	−2	1	−20	$=0$
z_2	1	−1	5	−1	1	−8	$=0$
1	1	6	−7	1	5	0	$=v$
	x_1	x_2	x_3	x_4	x_5	$=u$	

Búsquese simultáneamente las soluciones de dos problemas. Despéjese primero los desconocidos z_1 y z_2. Despejando z_2 para transformación con el elemento pivote 1 (note los caracteres en negrita) entonces

	y_1	y_2	y_3	y_4	0	1	
z_1	4	−3	8	−1	−1	−12	$=0$
x_5	1	−1	5	−1	1	−8	$=-y_5$
1	−4	11	−32	6	−5	40	$=v$
	x_1	x_2	x_3	x_4	z_2	$=u$	

Ahora atráigase z_2 por transformación con el elemento pivote 4 dela primera columna:

	0	y_2	y_3	y_4	0	1	
x_1	1/4	−3/4	2	−1/4	−1/4	−3	$=-y_1$
x_5	−1/4	−1/4	3	−3/4	5/4	−5	$=-y_5$
1	1	8	−24	5	−6	28	$=v$
	z_1	x_2	x_3	x_4	z_2	$=u$	

La primera y la quinta columna muestran que $z_1\ y\ z_2$ se expresan en función de $x_1\ y\ x_5$ de la siguiente manera:

(**III**)

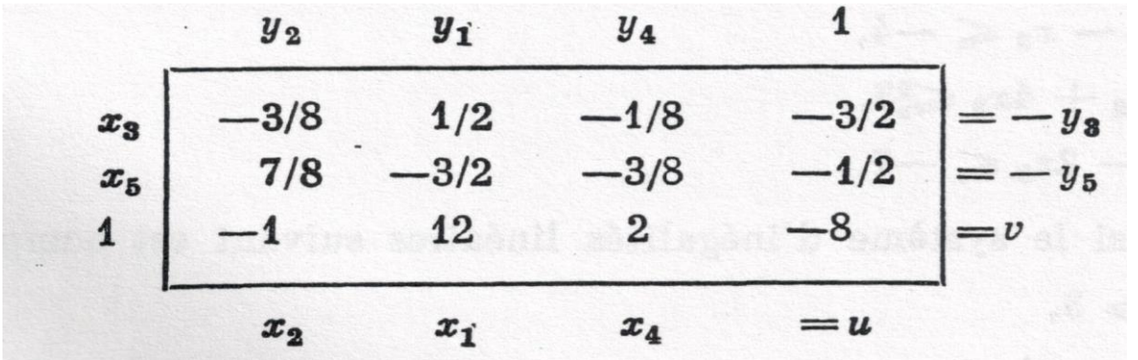
$$Z_1 = \tfrac{1}{4}x_1 - \tfrac{1}{4}x_5 + 1;$$

$$Z_2 = -\frac{1}{4}x_1 + \frac{5}{4}x_5 - 6.$$

Al eliminar la primera y la quinta columna en la tabla anterior, se tiene

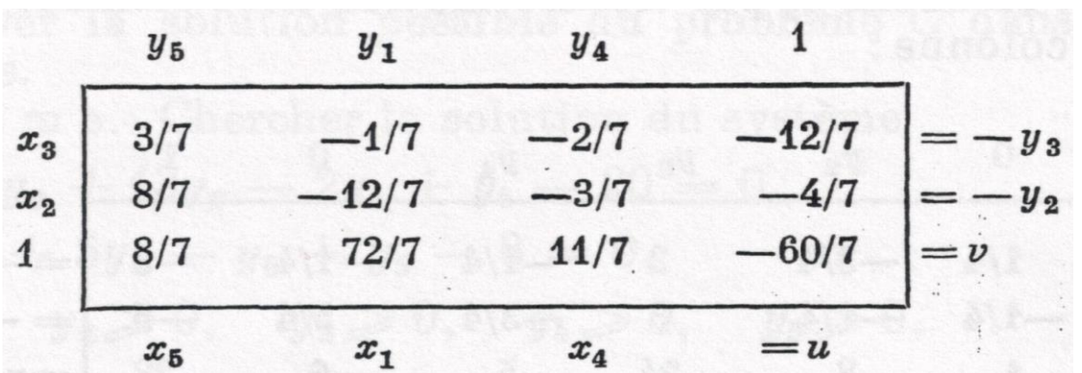
	y_2	y_3	y_4	1	
x_1	−3/4	2	−1/4	−3	$=-y_1$
x_5	−1/4	3	−3/4	−5	$=-y_5$
1	8	−24	5	28	$=v$
	x_2	x_3	x_4	$=u$	

Esta tabla es posible para filas. De acuerdo a la regla de elección del elemento pivote, se adopta 2 en la segunda columna, y al realizar la transformación se obtiene la tabla



	y_2	y_1	y_4	1	
x_3	−3/8	1/2	−1/8	−3/2	$= -y_3$
x_5	7/8	−3/2	−3/8	−1/2	$= -y_5$
1	−1	12	2	−8	$= v$
	x_2	x_1	x_4	$= u$	

En la tabla anterior el elemento 7/8 en la primera columna en vez del elemento pivote y se realiza la transformación, se obtiene la tabla



	y_5	y_1	y_4	1	
x_3	3/7	−1/7	−2/7	−12/7	$= -y_3$
x_2	8/7	−12/7	−3/7	−4/7	$= -y_2$
1	8/7	72/7	11/7	−60/7	$= v$
	x_5	x_1	x_4	$= u$	

Esta tabla es posible tanto para filas como para columnas. Al suponer las variables <<libres >> $x_2,\ x_3,\ y_1,\ y_4,\ y_5,$ es igual a cero, se tiene:

$x_1 = 72/7\ \ x_2 = 0, x_3 = 0, x_4 = 11/7\ x_5 = 8/7,$

$y_1 = 0, y_2 = {}^{4}/_{7}, y_3 = {}^{12}/_{7}, y_4 = 0, y_5 = 0.$

Al llevar los valores encontrados $x_1\ y\ x_5$ en las fórmulas (III), se obtiene $z_1 = 23/7,\ z_2 = -50/7$. Por lo tanto el vector (0, 4/7, 12/7, 0, 0) es la solución del primer problema mientras que el vector (23/7, $-50/7$) es la solución del problema dual. Además, $u = v = -50/7,$ es decir que el valor mínimo de la forma lineal v, y el valor máximo de la forma lineal u, son iguales $(-60/7)$.

Ejercicios

1. Maximizar la forma lineal $2_{x1} + 3_{x2}$ reemplazando las condiciones $4_{x1} + 2_{x2} + x_3 = 4$ y $x_1\ 3_{x2} = 5$.
2. Maximizar la forma lineal $x_1\ 3_{x2} + x_3$ reemplazando las condiciones
   $5_{x1} + 3_{x2} \leqslant 3, \quad x_1 + 2_{x2} + 4_{x3} \leqslant 4.$
3. Resolver el problema de la compatibilidad del sistema de inecuaciones lineales.

$$5x_1 + 4_{x2} - 7_{x3} \leqslant 1,$$

$$-x_1 + 2_{x2} - x_s \leqslant -4,$$

$$-3_{x_1} - 2x_2 + 4x_3 \leqslant 3,$$

$$3_{x_1} - 2x_2 - 2x_3 \leqslant -7.$$

4. Establecer si el siguiente sistema de desigualdades lineales es compatible:

$$4_{x1} - 5x_2 \geqslant 3,$$

$$-\ 2_{x1} -\ 7x_2 \geqslant 1,$$

$$-2_{x1} + x_2 \geqslant -2.$$

5. El sistema de ecuaciones lineales.

$$3_{x_1} - 5x_2 + 2x_3 = 0,$$

$$2_{x1} - 4x_2 + x_3 = 0$$

admite las soluciones no negativas no nulas?

6. Demostrar que el sistema de inecuaciones lineales

$$5x_1 - 4x_2 \leqslant 7,$$

$$-\ 3_{x1} + 3x_2 \leqslant -5$$

no tiene soluciones no negativas

7. Buscar las soluciones no negativas del sistema de ecuaciones lineales:
   $5x_1 + x_2 + 6_{x3} - 5x_5 = 2;$

   $-7x_1 - x_2 + 2_{x3} + x_4 + 2_{x5} = -5.$

CAPITULO X
GRUPOS
§ 1. Semi-grupo y monoides

Semi-grupos. Sea A un conjunto no vacío. La operación binaria $*$ en el conjunto A se denomina asociativa si $a * (b * c) = (a * b) * c$ para todos los elementos a, b, c de A. La operación binaria $*$ se denomina conmutativa si para cualesquiera a, b, c de A, se tiene $a * b = b * a$.

Es así que las operaciones de adición y de multiplicación de enteros son asociativas y conmutativas. Sin embargo, la operación de sustracción de enteros no es ni asociativa ni conmutativa.

DEFINICIÓN. Se denomina *Semi-grupo* al algebra $< A, * >$ del tipo (2) a la operación binaria asociativa$*$. Una sub-álgebra de un Semi-grupo se denomina *sub-semi-grupo.*

Ejemplos. 1. Sea $+$ una operación de adición en el conjunto N de números naturales. El algebra $< N, + >$ es un Semi-grupo, debido a que la operación de adición es asociativa. Este Semi-grupo se dice Semi-grupo aditivo de números naturales.

2. Sea M un conjunto no vacio y A la colección de todas las aplicaciones del conjunto M dentro de él mismo con la ley de composición de aplicaciones $\circ$ por medio de la operación binaria. El álgebra $< A, \circ >$ es un Semi-grupo, debido a que la operación de aplicaciones es asociativa- Este Semi-grupo es conocido como Semi-grupo de aplicaciones de conjunto M dentro de sí mismo.

Monoides. Sea A un conjunto de operaciones binaria $*$. El elemento e de A se dice elemento neutro en comparación a la operación $*$ si $a * e = e * a = a$ para todo a de A.

DEFINICIÓN. Se denomina monoide al algebra $< A, *, e >$ del tipo $(2, 0)$, cuyas operaciones principales satisfacen las condiciones siguientes:

(1) La operación binaria $*$ es asociativa;

(2) El elemento e es un elemento neutro en comparación a la operación$*$.

Ejemplos. 1. Sea $+$ una operación de adición en el conjunto N de los números naturales. El álgebra $< N, +, 0 >$ es un monoide, debido a que la adición es asociativa y 0 es un elemento neutro con respecto a la adición. Este monoide es conocido como monoide aditivo de números naturales.

2. Sea $\cdot$ la operación de multiplicación en el conjunto N de números naturales. El álgebra $< N, \cdot, 1 >$ es un monoide, debido a que la multiplicación es asociativa y 1 es un elemento neutro con respecto a la multiplicación. Este monoide se conoce como monoide multiplicativo de números naturales.

3. Sean n un número natural fijo diferente de cero, A la colección de todas las aplicaciones del conjunto $\{1, \dots, n\}$ dentro de si miso y E una aplicación idéntica de este conjunto. El álgebra $< A, \circ, E >$, donde $\circ$ es una operación binaria (conposicion de aplicaciones), es un monoide, debido a que la composición de aplicaciones es asociativa y E es un elemento neutro con respecto a la operación$\circ$. Este monoide se llama *monoide de aplicaciones del conjunto* $\{1, \dots, n\}$ *en sí mismo*.

4. Sea $\mathcal{K} = < K, +, -, \cdot, 1 >$ un anillo. El algebra $< K, \cdot, 1 >$ es entonces un monoide. Se le conoce como monoide multiplicativo de anillo $\mathcal{K}$.

Ley asociativa generalizada. Sea A un conjunto no vacio y $*$ una operación binaria en este último. Sea $a_1, a_2, \dots, a_n$ una sucesión de n elementos de A. Desígnese por el símbolo

$$a_1 * a_2 * \dots * a_n.$$

la *composición* de la sucesión de *elementos* definida de la manera inductiva siguiente:

$$a_1 * \ \ldots * a_{n-1} * \ a_n = (a_1 * \ldots * \ a_{n-1}) * \ a_n.$$

Según esta definición,

$$a * \mathrm{b} * \mathrm{c} = (\mathrm{a} * \mathrm{b}) * \mathrm{c}; \qquad \mathrm{a} * \mathrm{b} * \mathrm{c} * \mathrm{d} = (\mathrm{a} * \mathrm{b} * \mathrm{c}) * \mathrm{d}.$$

Si la ley de composición es una multiplicación, la composición de elementos $a_1, \ldots, a_n$ se denomina entonces *producto* y se dénota comúnmente $\prod_{1=1}^{n} a_1$; en caso de una notación aditiva de la composición de elementos $a_1, \ldots, a_n$ ella porta el nombre de *suma* y es comúnmente denotado$\sum_{i=1}^{n} a_i$.

Si la operación binaria * en el conjunto A es asociativa, se demuestra fácilmente que

$$a * b * c * d = (a * b) * (c * d) =$$

$$= a * (b * c) * d =$$

$$= (a * b * c) * d =$$

$$= a * (b * c * d).$$

En caso de que una operación binaria asociativa en A, el estudio de una composición cualquiera de una sucesión de elementos de A puede ser realizado mediante la colocación de paréntesis de cualquier manera, como lo muestra el TEOREMA siguiente.

TEOREMA 1.1. *Sean A un conjunto de operaciones binarias asociativo $*$ y $a_1, \ldots, a_n$ una sucesión del elementos de A. Sean $1 < n_1 < n_2 < \cdots < n_{\mathcal{K}} \leq n$, donde $n_1, \ldots, n_{\mathcal{K}}$ son números naturales, y $b_0 = a_1 * \ldots * a_{n1-1}$, $b_1 = a_{n1} * \ldots * a_{n2-1}, \ldots, b_R = a_{nR} * \ldots * a_n$,*

donde $a_1 * \ldots * a_n = b_0 * \ldots * b_R$.

Demostración (se efectúa por recurrencia sobre n). Si $n = 2$, el TEOREMA es aparentemente cierto. Supóngase que el TEOREMA es cierto si la sucesión comprende al menos $n - 1$ elementos como máximo.

Primer caso: $n_k = n$. En este caso $b_k = a_n$. Por definición,

$$a_1 * \ldots a_n = (a_1 * \ldots a_{n-1}) * a_n.$$

Por hipótesis de recurrencia,

$$a_1 * \ldots a_{n-1} = b_0 * \ldots * b_{R-1};$$

Por consiguiente,

$$a_1 * \ldots a_n = (b_0 * \ldots b_{R-1}) * b_R = b_0 * \ldots * b_R.$$

Segundo caso: $n_k < n$. En este caso

$b_R = (a_{n_R} * \ldots a_{n-1}) * a_n = b'_R * a_n$,

Donde $b'_R = a_{nR} * \ldots * a_{n-1}$ y

$a_1 * \ldots * a_{n-1} = b_0 * \ldots * b'_R$.

(según la hipótesis de inducción); por consiguiente,

$a_1 * \dots\ a_n = (\ a_1 * \dots\ a_{n-1}) *\ a_n =$

$= (\ b_0 * \dots *\ b'_R\ ) *\ a_n =$ (Por hipótesis de inducción)

$= \big((\ b_0 * \dots * b_{R-1}) *\ b'_R\big) *\ a_n =$

$= (\ b_0 * \dots * b_{R-1}) * (\ b'_R *\ a_n) =$

$= (\ b_0 * \dots * b_{R-1}) *\ b_R =$

$= b_0 * \dots * b_R$. □

Considérese el caso especial en el que la operación asociativa binaria sobre el conjunto A es una multiplicación y $a_1 =\ a_2 = \cdots =\ a_n = a$, en donde $a\ \in A$. Entonces, por definición,

$a^n =\ a_1 \cdot a_2 \dots\ a_n =\ \prod_{1=1}^{n}\ a_1$

COROLARIO 1.2 *Sean A un conjunto con una operación binaria asociativa de multiplicación dada sobre A y $a\ \in A$. Así que, para todos los números naturales m y n diferentes de cero*, se tiene:

$$a^{m+n} =\ a^m a^n, \qquad a^{mn} = (a^m)^n.$$

Considérese de igual manera el caso donde la operación binaria asociativa sobre el conjunto A es una adicion y $a_1 =\ \ a_2 = \cdots =\ \ a_n = a,$ donde $a\ \in A$. Así que por definición,

$$na =\ a_1 +\ a_n = \sum_{i=1}^{n} a_i.$$

COROLARIO 1.3. Sean A un conjunto con operación binaria asociativa de adición dada sobre A y $a\ \in A$. Entonces,

$(m+n)\ a = ma + na, \quad (mn)\ a = m\ (na),$
para todos los números naturales n y m diferentes de cero.

Ejercicios

1. Sea $< A,\ \cdot, 1 >$ un monoide multiplicativo. Demostrar que para todo elemento a del monoide y m y n números naturales cualesquiera, se tiene las relaciones
$$a^m a^n =\ a^{m+n}, \quad (a^m)^n =\ a^{mn}.$$
2. Sean $< A, +, 0 >$ un monoide aditivo y $a\ \in A$. Demostrar que para todos m y n naturales, se tiene
$$ma + na = (m+n)a, \quad n\ (ma) = (nm)\ a.$$
3. Sea $< N, +>$ un semi-grupo aditivo de números naturales. Buscar el sistema de generadores de este semi-grupo.
4. Sea $< N, +, 0 >$ un monoide aditivo de números naturales. Describir todos los submonoides de este monoide.
5. Sea $< N *,\ \cdot>$ un Semi-grupo multiplicativo de números naturales diferentes de cero. Buscar el sistema minimal de generadores de este Semi-grupo.
6. Sea $< N,\ \cdot>$ un Semi-grupo multiplicativo de números naturales. Buscar el sistema de generadores del Semi-grupo contenido en todo otro sistema de generadores de este Semi-grupo.

§ 2. Sub-grupos y categorías que siguen a un sub-grupo

Sub-grupos. Sean M un conjunto no vacío y S_M un conjunto de todas las permutaciones del conjunto M, es decir, la colección de todas las aplicaciones inyectivas del conjunto M sobre el mismo. Si f y g son permutaciones del conjunto M, su composición $f \circ g$ y la aplicación inversa f^{-1} son entonces permutaciones del conjunto M.

TEOREMA 2.1. El algebra $\langle S_M, \circ, ^{-1} \rangle$es un grupo.

Demostración. La operación binaria $\circ$ sobre S_M, composición de permutaciones del conjunto M, es asociativa en virtud del TEOREMA 2.2. La permutación idéntica i_M es un elemento neutro con respecto a la operación $\circ$. Para cualquier permutación f del conjunto $M, f \circ f^{-1} = i_M$. Por lo tanto, el algebra $\langle S_M, \circ, ^{-1} \rangle$es un grupo. □

DEFINICIÓN. El grupo $\langle S_M, \circ, ^{-1} \rangle$se denomina *grupo simétrico* en el conjunto M y se denota $\mathcal{P}_M$. Si el conjunto M es finito y comprende n elementos, el grupo $\mathcal{P}_M$ es conocido como el *grupo simétrico* de grado n y denotado $\mathcal{P}_n$.

Sea $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$un grupo multiplicativo. Para cada elemento a del grupo se asocia la aplicación t_a del conjunto G en G definido por la formula

$t_a(x) = ax$ para todo x de G.

La aplicación t_a es una permutación del conjunto G y se denomina *traslación a la derecha de* G. El conjunto G. El conjunto $T(G) = \{t_a \mid a \in G\}$ se denomina *conjunto de las traslaciones a la derecha de* G.

PROPOSICIÓN. 2.2. Sea $\mathcal{S}_G = \langle < S_G, \circ, ^{-1} \rangle$un grupo simétrico en el conjunto G. El algebra $\mathcal{T} = \langle T(G), \circ, ^{-1} \rangle$es un subgrupo del grupo $\mathcal{S}_G$.

Demostración. Para todos los elementos a, b del grupo $\mathcal{G}$ se tiene las igualdades.

(1) $t_a \circ t_b = t_{ab}$ y $t_a \circ t_a^{-1} = i_G = t_e$,

donde e es la unidad del grupo $\mathcal{G}$. En efecto, para todo x de G
$(t_a \circ t_b)(x) = t_a(t_b(x)) = t_a(bx) = abx = t_{ab}(x)$, es decir $t_a \circ t_b = t_{ab}$.

Al plantear en la última igualdad $b = a^{-1}$, se deduce $t_a \circ t_a^{-1} = t_e = i_G$, donde e es la unidad del grupo $\mathcal{G}$. Ademas, en virtud de (1) $t_a \circ t_e = t_{ae} = t_a$ y

(2) $(t_a)^{-1} = t_a^{-1} \in T(G)$.

Sobre la base de (1) y (2) se concluye que el conjunto $T(G)$ es cierra relativamente en las operaciones principales del grupo $S(G)$. Por consiguiente, el algebra $\langle T(G), \circ, ^{-1} \rangle$ es un subgrupo del grupo S_G. □

TEOREMA 2.3 (DE CAYLEY). *Todo grupo* $\mathcal{G} = \langle G, \circ, ^{-1} \rangle$ *es isomorfo al subgrupo del grupo simétrico en el conjunto* G. *En especial, cada grupo finito del orden* n *es isomorfo al subgrupo del grupo simétrico de grado* n.

Demostración. Sea $T(G)$ la colección de todas las traslaciones a la izquierda del conjunto G. Según el TEOREMA 2.2, el grupo $\mathcal{T} = \langle T(G), \circ, ^{-1} \rangle$ es un subgrupo del grupo $\mathcal{S}_G$.

Sea h una aplicación del conjunto G sobre $T(G)$ definido por la formula

$h(a) = t_a$ para todo a de G.

La aplicación h respeta las operaciones principales del grupo $\mathcal{G}$. Ciertamente, en virtud de (1) y (2), se tiene
$h(ab) = t_{ab} = t_a \circ t_b = h(a) \circ h(b)$,
$h(a^{-1}) = t_{a-1} = (t_a)^{-1} = (h(a =))^{-1}$.

Además, h es una aplicación inyectiva, De hecho, para todos a, b del conjunto G si $h\,(a) = h\,(b)$, se tiene $t_a = t_b$, $t_a\,(l) = t_b\,(e)$, donde e es la unidad del grupo $\mathcal{G}$, $ae = be$, y, en por consiguiente, $a = b$. Por lo tanto, h es un isomorfismo del grupo $\mathcal{G}$ en el subgrupo $\mathcal{T}$ del grupo simétrico S_G en el conjunto G. □

Categorías según un sub-grupo. Sea $\mathcal{H} = \langle H, \cdot, ^{-1} \rangle$ un subgrupo del grupo $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$. Introdúzcase en el conjunto G la relación binaria ≡ :

$a \equiv b$ (mod H) si y sólo si $ab^{-1} \in H$; llamese esta relación congruencia seguida al sub-grupo $\mathcal{H}$.

PROPOSICIÓN 2.4. *Sea $\mathcal{H}$ un sub-grupo del grupo $\mathcal{G}$. La congruencia en G seguida al subgrupo $\mathcal{H}$ es una relación de equivalencia.*

Demostración. Debido a que $aa^{-1} \in H$, se tiene $a \equiv a$ (mod H), es decir que la congruencia seguida a $\mathcal{H}$ es reflexiva. Puesto que $ab^{-1} \in H$ sigue $ba^{-1} \in H$, de $a \equiv b$ (mod H) sigue $b \equiv a$ (mod H): la congruencia siguiente $\mathcal{H}$ es simetrica. Por consiguiente, para todos los elementos a, b, c de G si $ab^{-1} \in H$ y $bc^{-1} \in H$, entonces $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. Por lo tanto, si $a \equiv b$ y $b \equiv c$ (mod H), entonces, $a \equiv c$ (mod H): la congruencia siguiente H es transitiva. Así, la congruencia siguiente $\mathcal{H}$ es una relación de equivalencia. □

Ejemplo. Sean $\langle V, +, - \rangle$ un grupo aditivo del espacio vectorial $\mathcal{V}$, $\mathcal{L}$ un sub-espacio del espacio $\mathcal{V}$ y $< L, +, - >$ su grupo aditivo. Considérese en V la relación binaria ∼ :

$a \sim b$ si y sólo si $a - b \in L$, se denomina *congruencia de vectores* de V *en sentido de* $\mathcal{L}$. Esta relación es una relación de equivalencia en V. Las categorías de equivalencia se denominan variedades lineales de espacio $\mathcal{V}$ en sentido $\mathcal{L}$.

DEFINICIÓN. Las categorías de equivalencia de la congruencia siguiente al sub-grupo $\mathcal{H}$ se denominan *categorías a la derecha del grupo $\mathcal{G}$ siguiente al sub-grupo $\mathcal{H}$*.

Nótese que las principales propiedades de las categorías siguen a un sub-grupo.

PROPIEDAD 2.1. *Ambas categorías a la derecha del grupo $\mathcal{G}$ siguen al subgrupo $\mathcal{H}$ sea coincidente sea sus disjuntos. El conjunto G es la reunión de todas las categorías a la derecha del grupo $\mathcal{G}$ seguido al sub-grupo $\mathcal{H}$*.

Esta propiedad resulta directamente del TEOREMA 2.4.1.

Sea $g \in G$. Notese que Hg es el conjunto definido por la igualdad $Hg = \{hg | h \in H\}$.

PROPIEDAD 2.2. *Si $g \in G$, entonces, Hg es una categoría a la derecha del grupo $\mathcal{G}$ que sigue al subgrupo $\mathcal{H}$*.

Demostración. Sea A la categoría a la derecha del grupo $\mathcal{G}$ que sigue al subgrupo $\mathcal{H}$ que contiene a g. Demuestrese $A = Hg$. Sea hg todo elemento de Hg. Entonces, $hgg^{-1} \in H$ y $hg \equiv g$ (mod H). Por lo tanto, $Hg \subset A$. Inversamente: si $c \in A$ es decir $c \equiv g$ (mod H), entonces, $cg^{-1} = h \in H$ y $c = hg \in Hg$. Por lo tanto, $A \subset Hg$. Por consiguiente, $A = Hg$. □

PROPIEDAD 2.3. Sean A la categoria a la derecho del grupo $\mathcal{G}$ que sigue al subgrupo $\mathcal{H}$ y $g \in A$, entonces, $A = Hg$.

Demostración. Las categorías A y Hg poseen un elemento común g. Según la propiedad 2.1. Estas coinciden, es decir $A = Hg$. □

PROPIEDAD 2.4. Sea $\mathcal{H}$ un subgrupo finito del grupo $\mathcal{G}$, $g \in G$. Entonces, el número de elementos de la categoría Hg vale el número de elementos del conjunto H.

Demostración. Sea m el número de elementos del conjunto H : $H = \{h_1, \dots, h_m\}$. Entonces, $Hg = \{h_1 g, \dots h_m g\}$ y $h_i g \neq h_R g$ para $i \neq k$, puesto que $h_i g = h_k g$, según la regla de simplificación, se seguiría la igualdad $h_i = h_{R.}$ Por consiguiente, el número de elementos del conjunto Hg de valor m.

Sea $\mathcal{H}$ el sub-grupo del grupo $\mathcal{G}$. Introduzcase en el conjunto G la relación binaria ∼ de la manera siguiente:

$a \sim b$ (mod H) si y sólo si $b^{-1}a \in H$; llamese la *congruencia a la izquierda que sigue al sub-grupo $\mathcal{H}$*. Una verificación directa muestra que esta relación es una equivalencia en el conjunto G. Las categorías de equivalencia de

esta relación se denominan *categorías a la izquierda del grupo* $\mathcal{G}$ que sigue al sub-grupo $\mathcal{H}$. Se verifica fácilmente que las categorías a la izquierda poseen propiedades análogas en las propiedades 2.1-2.1

TEOREMA de Lagrange. Sea $\mathcal{G}$ un grupo finito. EL número de elementos de su conjunto de base G es denominado orden de grupo $\mathcal{G}$.

TEOREMA 2.5. (de Lagrange). *El orden de subgrupo de un grupo finito es un divisor del orden del grupo.*

Demostración. Sean $\mathcal{H}$ un subgrupo del grupo finito $\mathcal{G}$ y

$H, Hg_2, \dots, Hg_k$

el conjunto de todas las categorías variadas a la derecha del grupo $\mathcal{G}$ que sigue al subgrupo $\mathcal{H}$. Entonces,

(1) $G = H \cup Hg_2 \cup \dots \cup Hg_{K,}$

adicionalmente, dos categorías cualesquiera incluida en esta reunión son disyuntivas. También, si n es el número de elementos del conjunto G y m el número de elementos del conjunto H se tiene, según la propiedad 2.4, que el número de elementos de toda categoría Hg_i vale m y, en virtud de (1), $n = mk$. □

COROLARIO 2.6. *Si* $\mathcal{G}$ *es un grupo finito de orden* n *y* $g \in G$, *entonces, el orden de elementos* g *divide* n.

COROLARIO 2.7. *Todo grupo finito de orden simple es cíclico.*

Ejercicios

1. Sea $\mathcal{S}_n = \langle S_n, \cdot, ^{-1} \rangle$ un grupo simétrico de permutaciones de grado n y A_n un conjunto de todas las permutaciones paras de S_n. Demostrar que $\mathcal{A}_n = \langle A_n, \cdot, ^{-1} \rangle$ es un sub-grupo del grupo $\mathcal{S}_n$.
2. Presentar que para un sub-grupo arbitrario de un grupo multiplicativo los elementos inversos de los elementos de la clase de la izquierda que constituyen los elementos de la clase de la derecha.
3. Demostrar que para $n > 1$ las $n - 1$ trasposiciones (12), (13),…, (1n) generando el grupo simétrico $\mathcal{S}_n$.
4. Presentar que para $n > 2$ los $n - 2$ ciclos a tres términos $(123), \dots, (12n)$ que genera el grupo $\mathcal{A}_n$ de permutaciones pares.
5. Sea $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ un grupo multiplicativo de matrices inversibles $n \times n$ en el cuerpo $\mathcal{F}$. Sea H un conjunto de todas las matrices de G cuyo determinante vale la unidad del cuerpo$\mathcal{F}$. Presentar que $\langle H, \cdot, ^{-1} \rangle$ es un sub-grupo del grupo $\mathcal{G}$.
6. Sean R^* un conjunto de todos los números reales diferente de cero y $\mathcal{R}^* = \langle R^*, \cdot, ^{-1} \rangle$ el grupo multiplicativo de números reales. Presentar que para cualquier número real $n \geq 1$ el grupo multiplicativo de raíces n-ésimas de la unidad es el único sub-grupo de orden n del grupo $\mathcal{R}^*$.

§ 3. Grupos cíclicos.

Orden de elemento de grupo. Sea $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ un grupo multiplicativo, e su elemento unidad y $a \in G$.

DEFINICIÓN. Se denomina orden de elemento a de grupo al más pequeño número natural m diferente de cero, tal como $a^m = e$. Si $a^n \neq e$ para todo número natural n no nulo, a es entonces conocido como elemento de orden infinito.

El orden de elemento a del grupo es denotado $\mathcal{O}(a)$.

Ejemplo: En un grupo multiplicativo de números complejos $\mathcal{O}(i) = \mathcal{O}(-1) = 2, \quad \mathcal{O}(1) = 1, \ \mathcal{O}(2) = \alpha$.

Se utilizará más adelante el TEOREMA siguiente (véase el TEOREMA 4.4.4. en la división con la resta).

Para los enteros n y $m > 0$ existe los enteros q y r, tales que

(1) $n = m \cdot q + r, \qquad 0 \leq r < m.$

TEOREMA 3.1. *Sea m un orden (finito= de elemento a de un grupo multiplicativo. La igualdad $a^n = e$, donde n es un entero, se verifica si y sólo si m divide a n.*

Demostración. Plantéese que $a^n = e$ y demuestrese que m divide a n. Según el TEOREMA de la división con la resta, existe para los números n y m de enteros q y r que satisfacen las condiciones (1). Se trata de demostrar que $r = 0$. En virtud de la condición $a^m = e$ y por hipótesis, $a^n = e$. En virtud de (1), se deduce que

$$a^n = a^{mq} \cdot a^r = (a^m)^q \cdot a^r = a^r = e.$$

Dado que $\mathcal{O}(a) = m$ y $0 \leq r < m$, se deduce $a^r = e$ que $r = 0$, es decir que m divide a n.

Supóngase ahora que m divide a n y demuestrese que $a^n = e$, m que divide a n, se tiene que $n = mk$ para un cierto entero K. Por lo tanto $a^n = a^{mk} = (a^m)^k = e^k = e$, es decir $a^n = e$. □

PROPOSICIÓN 3.2. *Sea a un elemento del grupo multiplicativo provisto de un orden finito m. La igualdad $a^r = a^s$, donde r y s son enteros, se verifica si y solo si m divide $r - s$.*

Demostración. La igualdad $a^r = a^s$ ocurre si y sólo si $a^{r-s} = e$. Según el TEOREMA 3.1, $a^{r-s} = e$ si y sólo si m divide $r - s$.

COROLARIO 3.3. Sea a un elemento del grupo multiplicativo provisto de un orden finito m. Sean r y s enteros; $\bar{r} = r + mZ$ y $\bar{s} = s + mZ$ son de categorías residuales módulo m. La igualdad $a^r = a^s$ se verifica si y sólo si $\bar{r} = \bar{s}$.

COROLARIO 3.4. Sea a un elemento de grupo multiplicativo provisto de un orden finito m. Los elementos $e = (a^0), a, a^2, \dots, a^{m-1}$ son entonces distintos.

PROPOSICIÓN 3.5. Sea a un elemento de grupo multiplicativo de orden finito y r, s enteros. La igualdad $a^r = a^s$ ocurre si y sólo si $r = s$.

Demostración. De la igualdad $r = s$ se obtiene aparentemente la igualdad $a^r = a^s$. Se establece $a^r = a^s$. Si $r \neq s$, por ejemplo, si $r > s$, entonces $a^{r-s} = e$ y $r - s \neq 0$. Esto es imposible, debido a que, por hipótesis, el elemento a posee un orden infinito. Por lo tanto, $r = s$. □

Grupos cíclicos. Se proporcionará más adelante la descripción de grupos cíclicos.

DEFINICIÓN. Un grupo multiplicativo (aditivo) es conocido como cíclico si el conjunto de basa del grupo es compuesto de potencias (múltiples) de un elemento cualquiera del grupo; este elemento es conocido como elemento generador del grupo.

Ejemplos. 1. Sea $\mathcal{Z} = \langle Z, +, - \rangle$un grupo aditivo de enteros. Cada elemento del grupo es multiplico de 1 (ó (-1)). Por consiguiente, $\mathcal{Z}$es un grupo cíclico de elemento generador 1 (ó (-1)).

2. El grupo de superposiciones en sí mismo de un polígono regular d m ángulos es un grupo cíclico de orden m. Una rotación de $2\pi/m$ de un polígono de m angulos alrededor del centro es un elemento generador de este grupo.

3. Sea m un entero positivo, $\bar{k} = k + mZ$ y $Z_m = \{\overline{0, 1, \dots, \overline{m-1}}\}$ un conjunto de todas las categorías residuales módulo m. La operación de adición $+$ y la operación singular $-$ se defininen asi:

$$\bar{k} + \bar{s}, \qquad -(\bar{k}) = \overline{(-k)} = \overline{(m-k)}.$$

La operación de adición es asociativa y conmutativa. $\bar{0}$ es igualmente neutro comparado a la adición de las categorías y $\bar{k} + (\overline{-k}) = 0$. Por consiguiente, el algebra $\mathcal{Z}_m = < Z_m, +, - >$ es un grupo conmutativo de orden m. Este es un grupo cíclico de elemento generador $\bar{1}$. El grupo $\mathcal{Z}_m$ es conocido como grupo aditivo de categorías residuales módulo m.

TEOREMA 3.6. Si el elemento generador de un grupo cíclico es provisto de un orden infinito, el grupo es entonces isomorfo en el grupo cíclico que posee un orden finito m.

Demostración. Sea $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ un grupo multiplicativo cíclico en el elemento generador a, es decir que $G = \{a^n | n \in Z\}$. Sea $\mathcal{Z} = \langle Z, +, - \rangle$un grupo aditivo de enteros y $\mathcal{Z} = \langle Z_m, +, - \rangle$ un grupo aditivo de categorías residuales módulo m.

Primer caso: $\mathcal{O}(a) = \alpha$. En este caso, en virtud de la proposición 3.5, todas las potencias enteras del elemento generador a son independientes. Por tanto, la aplicación f del conjunto G en Z tal como $f(a^n) = n$ para todo n entero es inyectivo. La aplicación f respeta las operaciones principales del grupo $\mathcal{G}$ debido a que para todos los enteros n y s:

$$f(a^n a^s) = f(a^{n+s}) = n + s = f(a^n) + f(a^s),$$
$$f(a^{-n}) = -n = -f(a^n).$$

Por consiguiente, f es una aplicación isomorfa del grupo $\mathcal{G}$ en el grupo $\mathcal{Z}$.

Segundo caso: $\mathcal{O}(a) = m$, el elemento a es provisto de un orden finito m. Muéstrese que en este caso el grupo $\mathcal{G}$ es isomorfo en el grupo $\mathcal{Z}_m$. Demuéstrese que $G = \{e, a, a^2, \dots, a^{m-1}\}$. Sea a^R un elemento cualquiera de G. Según el TEOREMA de división con resta, existe para los números k y m de los enteros q y r tales que

$$k = mq + r, \quad 0 \leq r < m.$$

Se deduce que

$$a^k = a^{mq} a^r = a^r \in \{e, a, \dots, a^{m-1}\};$$

Por consiguiente,

$$G = \{e, a, \dots, a^{m-1}\}.$$

Considérese la aplicación φ del conjunto G en el conjunto Z_m:

$Z_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ tal que

$$\varphi(a^k) = \bar{k} \quad \text{para } k = 0, 1, \dots, m-1.$$

En virtud de la proposición 3.2, φ es una aplicación inyectiva del conjunto G en Z_m. Adicionalmente, φ respeta las operaciones principales del grupo $\mathcal{G}$, de modo que

$$\varphi(a^k a^s) = \varphi(a^{k+s}) = \overline{k+s} = \bar{k} + \bar{s} = \varphi(a^k) + \varphi(a^s),$$
$$\varphi(a^{-k}) = \overline{m-k} = -(\bar{k}).$$

Por consiguiente, φ es una aplicación isomorfa del grupo $\mathcal{G}$ en el grupo $\mathcal{Z}_m$. □

Sub-grupos de grupo cíclico. Preséntese que todo subgrupo de grupo cíclico es también cíclico.

TEOREMA 3.7. Todo subgrupo de grupo cíclico es un grupo cíclico.

Demostración. Sea $\mathcal{G}$ un grupo multiplicativo cíclico de elemento generador a. Sea $\mathcal{H}$ el subgrupo de grupo $\mathcal{G}$. El TEOREMA es aparentemente cierto si H comprende solo un elemento. Supóngase que H comprendiera más de un elemento. El sub-grupo $\mathcal{H}$ contiene al menos una potencia negativa de elemento a debido a, de otra forma, si $a^{-k} \in H$, entonces $(a^{-k})^{-1} = a^k \in H$. Sea a^s un elemento de H con un exponente positivo un poco más pequeño de la potencia s. Cualquier elemento de H es una elemento de aspecto a^k. Si $a^k \in H$, entonces s divide a k. De hecho, según el TEOREMA de división con resta (TEOREMA 4.4.4.) existe para los números k y s de los enteros q y r tales que

(1) $K = sq + r$ y $0 \leq r < s$.

En razón de (1), $a^r = a^{R-sq} = a^R(a^s)^{-q} \in H$. Como $a^r \in H$ y $0 \leq r < s$, en virtud de la elección de número $s, r = 0$; por lo tanto $K = sq$. El conjunto H esta también compuesto de potencias de elemento a^s. Por consiguiente, $\mathcal{H}$ es un grupo cíclico de elemento generador a^s. □

Ejercicios

1. Buscar todos los sub-grupos del grupo aditivo $\mathcal{L}$ de todos los enteros.
2. Buscar todos los sub-grupos del grupo cíclico de orden 12.
3. Buscar todos los sub-grupos del grupo cíclico de orden 24.
4. Demostrar que un grupo finito de orden simple es cíclico y que su elemento cualquiera, difiere del elemento neutro, y es el elemento generador.
5. Demostrar que existe grupos cíclicos de orden arbitrario.
6. Demostrar que el orden de un elemento cualquiera de un grupo finito es un divisor del orden de grupo.
7. Sea m y n números naturales primos entre ellos. Mostrar que en un grupo abeliano multiplicativo el producto de un elemento a de orden m por un elemento b de orden n ese es un elemento de orden mn.
8. Mostrar que todo grupo de orden 15 es cíclico.
9. Sea $\mathcal{G}$ un grupo multiplicativo de raíces de 1 (raíces de potencia n para los números naturales cualesquiera $n > 0$). Presentar que para todo número natural m diferente de cero, el grupo $\mathcal{G}$ no posee más que un solo subgrupo de orden m y que cada uno de estos subgrupos es cíclico.

§ 4. Divisores normales y grupos cocientes.

Divisores normales de grupo. Sea $\mathcal{H}$ un subgrupo del grupo $\mathcal{G}$. Una pregunta surge naturalmente: ¿A qué condiciones se rigen las particiones del conjunto G en categorías a la derecha y a la izquierda que siguen al subgrupo $\mathcal{H}$ coincidente? Los subgrupos provistos de estas propiedades son distinguidos a través de la siguiente definición.

DEFINICIÓN: Un subgrupo $\mathcal{H}$ del grupo $\mathcal{G}$ se denomina *divisor normal de grupo* $\mathcal{G}$ si $g^{-1}hg \in H$ para cualquier elemento g de G y cualquier elemento h de H.

La notación $\mathcal{H} \lhd \mathcal{G}$ significa que $\mathcal{H}$ es un divisor normal del grupo $\mathcal{G}$.

Ejemplos. 1. Sea $\mathcal{S}_n$ un grupo simétrico de permutaciones de grado n y $\mathcal{A}_n$ son sub-grupos de todas las permutaciones pares. Entonces $\mathcal{A}_n \lhd \mathcal{S}_n$.

2. Cualquier sub-grupo de un grupo abeliano es su divisor normal.

3. Sea $\mathcal{G}$ un grupo multiplicativo de matrices inversibles $n \times n$ en el cuerpo $\mathcal{F}$ y $\mathcal{H}$ un subgrupo de matrices cuyos determinantes son iguales a la unidad. Entonces $\mathcal{H} \lhd \mathcal{G}$.

Véase algunas propiedades de divisores normales de grupo.

PROPIEDAD 4.1. El sub-grupo $\mathcal{H}$ del grupo $\mathcal{G}$ es un divisor normal del grupo $\mathcal{G}$ si y sólo si cada categoría a la derecha del grupo $\mathcal{G}$ que sigue el sub-grupo $\mathcal{H}$ es igualmente una categoría de la derecha.

Demostración. Plantéese

(1) $\mathcal{H} \lhd \mathcal{G}$,

y demuéstrese que

(2) $Hg = gH$ para todo g de G.

En virtud de (1), $g^{-1}hg \in H$ para todo h de H. Así tan bien se obtiene $hg \in gH$ y $Hg \subset gH$. Entonces, en virtud de (1), $(g^{-1})^{-1}hg^{-1} \in H$. Por consiguiente, $gH \in Hg$ para todo h de H, es decir se esta en presencia de una inclusión $gH \subset Hg$. Así, de (1) resulta (2).

Supóngase ahora que se cumple la condición (2). Entonces, para todo $h \in H$ existe un $h_1 \in H$ tal como $hg = gh_1$. Por consiguiente, $g^{-1}hg \in H$ para todo $g \in G$ y todo $h \in H$, es decir $\mathcal{H} \lhd \mathcal{G}$. Por lo tanto de (2) se deduce (1). □

PROPIEDAD 4.2. Sea $\mathcal{A}$ un subgrupo del grupo $\mathcal{B}, \mathcal{B}$ siendo un subgrupo del grupo $\mathcal{G}$ y $\mathcal{A} \lhd \mathcal{B}$, entonces $\mathcal{A} \lhd \mathcal{B}$.

Demostración. Sean a y b elementos cualesquiera de $|\mathcal{A}|$ y $|\mathcal{B}|$ respectivamente. Entonces, $b^{-1}ab \in |\mathcal{A}|$, entonces por hipótesis, $\mathcal{A} \lhd \mathcal{G}$. Por lo tanto $\mathcal{A} \lhd \mathcal{B}$.□

PROPIEDAD 4.3. Una intersección de cualquier colección de divisores normales de grupo $\mathcal{G}$ es un divisor normal del grupo $\mathcal{G}$.

Demostración. Sean $\mathcal{A} \lhd \mathcal{B}$ y $\mathcal{B} \lhd \mathcal{G}$. Entonces, $\mathcal{A} \cap \mathcal{B}$ es un sub-grupo del grupo $\mathcal{G}$. Si $c \in |\mathcal{A}| \cap |\mathcal{B}|$ y $g \in G$, entonces

$$g^{-1}cg \in |\mathcal{A}|, \qquad g^{-1}cg \in |\mathcal{B}|,$$

Dado que $\mathcal{A}$ y $\mathcal{B}$, por hipótesis, son divisores normales del grupo $\mathcal{G}$. Por lo tanto $g^{-1}cg \in |\mathcal{A}| \cap |\mathcal{B}|$ y $|\mathcal{A}| \cap |\mathcal{B}| \lhd \mathcal{G}$.

De manera análoga, se demuestra la propiedad 4.3 se reproduce para cualquier colección de divisores normales del grupo $\mathcal{G}$. □

Grupo cociente. Sea $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ un grupo multiplicativo y $A, B \subset G$. Defínase el producto $A \cdot B$ de conjuntos A y B por la formula

$$A \cdot B = \{x \cdot y | x \in A, y \in B\}.$$

PROPOSICIÓN 4.1. *Sean $\mathcal{H}$ un divisor normal del grupo $\mathcal{G}$ y G/H el conjunto de todas las categorías del grupo $\mathcal{H}$. El producto de dos categorías cualesquiera del grupo $\mathcal{G}$ que siguen a $\mathcal{H}$ es una categoría que sigue a un sub-grupo. Además,*

$$Ha \cdot Hb = Hab.$$

Demostración. Sea ha y $h_1 b$, donde $h, h_1 \in H$, de elementos cualesquiera de Ha y Hb respectivamente. En este caso, $ah_1 a^{-1} \in H$ puesto que $\mathcal{H} \lhd \mathcal{G}$. Por lo tanto,

$$ha \cdot h_1 b = h\,(ah_1 a^{-1})\,ab \in Hab;$$

Por consiguiente, $(Ha) \cdot (Hb) \subset Hab$.

Demuéstrese la inclusión inversa. Sea $hab \in Hab$. Entonces, $hab = (ha)b \in Ha \cdot Hb$. Por lo tanto $Hab \subset (Ha) \cdot (Hb)$; por consiguiente, $(Ha) \cdot (Hb) = Hab$, □

Defínase en el conjunto G/H las operaciones $\cdot$ y $^{-1}$ para las fórmulas

$$(Ha) \cdot (Hb) = Hab, \qquad (Ha)^{-1} = Ha^{-1}$$

y considérese el algebra

$$\frac{\mathcal{G}}{\mathcal{H}} = \langle G/H, \cdot, ^{-1} \rangle$$

TEOREMA 4.2. Sea $\mathcal{H}$ un divisor normal del grupo $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$. El algebra $\frac{\mathcal{G}}{\mathcal{H}} = \langle G/H, \cdot, ^{-1} \rangle$ es un grupo.

Demostración. Sea $Ha, Hb \in G/H$. Las operaciones en G/H son definidas por las igualdades

(1) $(Ha) \cdot (Hb) = Hab, \quad (Ha)^{-1} = Ha^{-1}$.

La operación de multiplicación de las categorías que siguen a un subgrupo es asociativa. De hecho, si $A = Ha, B = Hbm\, c = Hc$, entonces, en virtud de (1),

$$A \cdot (B \cdot C) = (Ha) \cdot (Hbc) = Habc,$$
$$(A \cdot B) \cdot C = (Hab) \cdot (Hc) = Habc.$$

Por tanto, $A(BC) = (AB)C$ para todos A, B, C de G/H.

El elemento H de G/H es un elemento unidad comparado a la multiplicación, debido a que $A \cdot H = Ha \cdot He = Ha = A$, es decir que $A \cdot H = A$ para todo A de G/H. En virtud de (1), $A \cdot A^{-1} = Ha \cdot Ha^{-1} = Haa^{-1} = H$ Para todo elemento A de G/H. Por consiguiente, el algebra $\mathcal{G}/\mathcal{H}$ es un grupo. □

DEFINICIÓN. El álgebra $\mathcal{G}/\mathcal{H}$ es conocida como grupo cociente del grupo $\mathcal{G}$ que sigue al sub-grupo $\mathcal{H}$.

Ejemplos. 1. Sea $\mathcal{Z}$ un grupo aditivo de enteros, m un número natural fijo y $\bar{k} = K + mZ$.

Entonces,

$$\frac{Z}{mZ} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$
$$\bar{k} + \bar{n} = \overline{k+n}, -(\bar{k}) = \overline{(-k)} = \overline{m-k}.$$

El algebra $\frac{\mathcal{Z}}{m\mathcal{Z}} = < \frac{Z}{mZ}, +, - >$ es un grupo cociente del grupo $\mathcal{Z}$ que sigue al subgrupo $m\mathcal{Z}$.

2. Sea $\mathcal{S}_n$ un grupo simétrico de permutaciones de grado n $(n > 1)$ y $\mathcal{A}_n$ son subgrupos de permutaciones pares. Entonces, el grupo cociente $\mathcal{S}_n/\mathcal{A}_n$ es un grupo cíclico de segundo orden, debido a que $S_n/A_n = \{A_n, A_n o\}$, donde o es una permutación impar.

Núcleo de un homomorfismo. Sean $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ y $\mathcal{G}' = \langle G', \cdot, ^{-1} \rangle$grupos multiplicativos.

DEFINICIÓN. Sea φ un homomorfismo de grupo $\mathcal{G}$ en el grupo $\mathcal{G}'$. Llámese núcleo de un homomorfismo φ al conjunto

$$Ker\ \varphi = \{x \in G | \varphi(x) = e'\},$$

donde e' es la unidad del grupo $\mathcal{G}'$.

El conjunto $Ker\ \varphi$ no es vacío, debido a que $\varphi(e) = e'$. El conjunto $Ker\ \varphi$ es cerrado en el grupo $\mathcal{G}$ debido a que para todos a, b de $Ker\ \varphi$ se tiene

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b) = e' \circ e' = e';$$

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e',$$

es decir que $a \cdot b$ y a^{-1} pertenecen al conjunto $Ker\ \varphi$.

DEFINICIÓN. Un sub-grupo $\mathcal{G}$ con conjunto de base $Ker\ \varphi$, donde φ es un homomorfismo de grupo $\mathcal{G}$, y se denotará $Ker\ \varphi$:

$$Ker\ \varphi = \langle Ker\ \varphi, \cdot, ^{-1} \rangle$$

y se le denominará *grupo del núcleo de un homomorfismo* φ o simplemente núcleo φ.

PROPOSICIÓN 4.3. *Si φ es un homomorfismo del grupo $\mathcal{G}$ en el grupo $\mathcal{G}'$, entonces $Ker\ \varphi$ es un divisor normal del grupo $\mathcal{G}$.*

Demostración. Anteriormente, se demostró que el conjunto $Ker\ \varphi$ es cerrado relativamente a las operaciones principales del grupo $\mathcal{G}$. Adicionalmente, para todo g de Gy todo h de $Ker\ \varphi$ se tiene

$$\varphi\ (g^{-1}hg) = \varphi(g^{-1}) \circ e' \circ \ddot{\varphi}\ (g) = \varphi\ (g^{-1}eg) = \varphi\ (e) = e'$$

Es decir $g^{-1}hg\ \in Ker\ \varphi$. Por consiguiente, $\mathcal{K}er\ \varphi$ es un divisor normal del grupo $\mathcal{G}$.

PROPOSICIÓN 4.4. *Sea φ un homomorfismo de grupo $\mathcal{G}$ en el grupo $\mathcal{G}'$ con anillo $\mathcal{H} = \langle H, \cdot, ^{-1} \rangle$. Para todo a, b de G, si $\varphi\ (a) = \varphi\ (b)$, se tiene $Ha = Hb$.*

Demostración. φ al ser un homomorfismo y $\varphi\ (a) = \varphi\ (b)$, se tiene

$$\varphi\ (ab^{-1}) = \varphi\ (a) \circ \varphi\ (b^{-1}) = \varphi\ (a) \circ \big(\varphi\ (b)\big)^{-1} = \varphi\ (a) \circ \big(\varphi\ (a)\big)^{-1} = e'$$

Por consiguiente, $a \cdot b^{-1}\ \in H$ y $Ha = Hb$. □

TEOREMA de homomorfismos. En la teoría de grupos el TEOREMA que sigue en los homomorfismos es uno de los principales.

TEOREMA 4.5. *Sea f un homomorfismo de grupo $\mathcal{G}$ en el grupo $\mathcal{G}'$ con núcleo $\mathcal{H}$. El grupo cociente $\mathcal{G}/\mathcal{H}$ es entonces isomorfo en el grupo $\mathcal{G}'$.*

Demostración. Sean $\mathcal{H} = \mathcal{K}er\ f$ y $H = Ker\ f$. Sea $|G| = G/H$ el conjunto de todas las categorías de grupo $\mathcal{G}$ que siguen al subgrupo$\mathcal{H}$. Considérese la aplicación

$$\varphi : G/H \to G',$$

definida de la siguiente manera:

(1) $\varphi\ (Ha) = f(a)$ para toda categoría que sigue en un subgrupo Ha de $|G|$.

Dado que $Ker\ f = H$, el valor de $\varphi\ (Ha)$ no depende de la selección de a en la categoría que sigue un subgrupo Ha.
La aplicación φ respeta la operación de multiplicación en el grupo $\mathcal{G}/\mathcal{H}$, debido a que

$$\varphi\ (Ha \cdot Hb) = \varphi\ (Hab) = f(a) \cdot f(b) = \varphi\ (Ha)\ \varphi(Hb).$$

Por lo tanto, según el TEOREMA 3.3.1, φ es un homomorfismo de grupo $\mathcal{G}/\mathcal{H}$ en $\mathcal{G}'$.
Por hipótesis, f es una aplicación de G en G'. En virtud de (1), se deduce que φ es una aplicación de G/H en G'. La aplicación φ es inyectiva. De hecho, en virtud de (1), de igualdad $\varphi\ (Ha) = \varphi\ (Hb)$ se deduce $f(a) = f\ (b)$; según la proposición 4.4, se deduce $Ha = Hb$. En resumen, se establece que φ es una aplicación inyectiva de G/H en G'. Por consiguiente, φ es un homomorfismo de grupo cociente $\mathcal{G}/\mathcal{H}$ en el grupo $\mathcal{G}'$. □

Ejercicios

1. Demostrar que cualquier grupo cociente de un grupo aditivo $\mathcal{L}$ de enteros es cíclico.
2. Buscar todos los grupos cocientes de un grupo cíclico de orden 12.
3. Demostrar que todo grupo cociente de un grupo cíclico es cíclico.
4. Demostrar que un grupo cociente de un grupo simétrico $\mathcal{S}_n$ de permutaciones de grado n que sigue al subgrupo $\mathcal{A}_n$ de todas las permutaciones pares, es un grupo cíclico de segundo orden.
5. Demostrar que el grupo aditivo $\mathcal{L}$ de enteros es isomorfo al grupo aditivo $2\mathcal{L}$ de números pares.
6. Demostrar que el grupo aditivo de todos los números complejos es isomorfo al grupo aditivo de todos los vectores del plano.
7. Sea $\mathcal{G}$ un grupo de permutaciones. Considérese la aplicación h del grupo $\mathcal{G}$ en el grupo multiplicativo de números $+1$ y -1 que asocia cada permutación τ $\mathcal{G}$ en su signatura sgn τ. Mostrar que h es un homomorfismo.
8. Mostrar que el grupo multiplicativo de raíces m-ésimas de 1 es isomorfa al grupo aditivo $\mathcal{L}_m$ de categorías residuales módulo m.
9. Sea $\mathcal{G}$ el grupo multiplicativo de matrices inversas y reales $n \times n$ y $\mathcal{R}^*$ que asocia cada elemento g del grupo $\mathcal{G}$ al determinante $|g|$. Demostrar que h es un homomorfismo cuyo núcleo es el sub-grupo del grupo $\mathcal{G}$ de todas las matrices $n \times n$ con determinantes iguales a 1.
10. Sean $\mathcal{R}$ un grupo aditivo de números reales y $\mathcal{K}$ un grupo multiplicativo de números complejos cuyo módulo vale 1. Demostrar que la aplicación f del conjunto R en K definido por la formula $f(x) = \cos 2\pi x + i \sin 2\pi x$ es un homomorfismo del grupo $\mathcal{R}$ en el grupo $\mathcal{K}$ con núcleo Z.
11. Sean $\mathcal{Q}$ un grupo aditivo de números racionales y $\mathcal{Z}$ un grupo aditivo de enteros. Mostrar que cada elemento del grupo cociente $\mathcal{Q}/\mathcal{Z}$ posee un orden finito. Demostrar que para todo n natural diferente de cero, $\mathcal{Q}/\mathcal{Z}\mathcal{Z}$ posee solamente un sub-grupo de orden n y que cada uno de estos sub-grupos es cíclico.

CAPITULO XI
TEORÍA DE DIVISIBILIDAD EN EL ANILLO DE ENTEROS.

§ 1. Descomposición de enteros en factores primos.

Ideales de un anillo de enteros. Introdúzcase la noción de un ideal.

DEFINICIÓN: un conjunto no vacío $\boldsymbol{I}$ de enteros se le denomina *ideal de un anillo* $\mathbb{Z}$ de enteros si es cerrado en relación a la adición y a la multiplicación en todos los enteros, es decir si $a + b, ma \in \boldsymbol{Z}$ para todos $a, b \in \boldsymbol{I}$ y todo $m \in \boldsymbol{Z}$.

Resulta de la definición que todo ideal I es cerrado en relación a la sustracción y, por consiguiente, que contiene el número cero.

Sea n un entero fijo cualquiera. Se verifica fácilmente que el conjunto $n\boldsymbol{Z}, n\boldsymbol{Z} = \{nx | x \in \boldsymbol{Z}\}$, es un ideal del anillo $\mathcal{Z}$. Este ideal se denomina *ideal principal* generado por el número n. El ideal $0.\boldsymbol{Z}$ se compone solamente de un cero y se le denomina *ideal nulo.* Se ve con facilidad que $n\boldsymbol{Z} = (-n)\boldsymbol{Z}$. El ideal generado por el número n igualmente se denota (n).

TEOREMA 1.1. *Cada ideal de un anillo de enteros es principal. Si* $\boldsymbol{I}$ *es un ideal no nulo del anillo* $\mathcal{Z}$ *y* d *el menor número positivo contenido en* $\boldsymbol{I}$*, el conjunto* $\boldsymbol{I}$ *se compone estrictamente de números múltiplos de* d*, es decir* $\boldsymbol{I} = d\boldsymbol{Z}$.

Demostración. El ideal nulo es evidentemente un ideal principal generado por un cero. Sea $\boldsymbol{I}$ un ideal no nulo, es decir que incluye al menos un número a diferente de cero. Entonces, $a, -a \in \boldsymbol{I}$ y uno de estos números es positivo. Sea d el menor número positivo contenido en $\boldsymbol{I}$. El ideal $\boldsymbol{I}$ incluye todos los múltiplos de d, es decir $d\boldsymbol{Z} \subset \boldsymbol{I}$. También debe mostrar que todo número c de I es múltiplo de d. Con este fin, se divide c por d con el residuo:

$$c = dq + r, \qquad 0 \leqslant r < d, \qquad q, r \in \boldsymbol{Z}.$$

Como c y dq pertenecen al ideal I, se obtiene $c - dq = r \in I$. El caso de $r > 0$ es imposible, en vista que d es el menor número positivo contenido en $\boldsymbol{I}$. Por consiguiente, $r = 0$ y $c = dq$. Así, el ideal I se compone estrictamente de múltiplos de $d, I = d\boldsymbol{Z}$.□

Números primos: El entero p se le denomina primo si es diferente de cero y de ± 1 y únicamente posee divisores ± 1 y $\pm p$. Un entero a diferente de cero y de ± 1 y que posea otros divisores que ± 1 y $\pm a$ se le denomina *número compuesto*.

Una verificación directa muestra que los primeros factores primos positivos son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29;$$

los primeros factores primos negativos son

$$-2, -3, -5, -7, -11, -13, -17, -19, -23, -29.$$

Factorización de números enteros: Los enteros a y b se les denomina *primos entre ellos* si cualquier divisor común de estos últimos es $+1$ o -1.

PROPOSICIÓN 1.2. *Si los enteros a y b son primos entre sí, existe entonces enteros u, v tales que $au + bv = 1$.*

Demostración. Considérese el conjunto

$$\boldsymbol{I} = \{ax + by | x, y \in \boldsymbol{Z}\}.$$

Se ve fácilmente que este conjunto es no vacío y es cerrado en relación a la adición y a la multiplicación por enteros. Por consiguiente $\boldsymbol{I}$ es un ideal del anillo $\mathcal{Z}$ de enteros. El conjunto $\boldsymbol{I}$ incluye el número $a, a = a.1 + b.0$ y el número $b: b = a.0 + b.1$. El conjunto $\boldsymbol{I}$ contiene números positivos, ya que a y b son son primos entre si, y por consiguiente, al menos uno de estos números es diferente de cero. Nótese d el menor número natural positivo pertenece al conjunto $\boldsymbol{I}$. Entonces, por definición del conjunto $\boldsymbol{I}$, existe enteros u, v tales que $au + bv = d$. Según el TEOREMA 4.4.5, d es un común divisor de los números a y b. a y b al ser primos entre si $d > 0$, resulta que $d = 1$. Así, $au + bv = 1$.□

TEOREMA 1.3. *Si el producto de dos enteros se divide por un número primo p, entonces al menos uno de los factores admite p para divisor*.

Demostración. Sea ab el producto de números enteros que admite p como divisor, a no se divide por p. a y p son entonces primos entre si. Según la proposición 1.2, existe enteros u, v tales que $au + pv = 1$, de donde

$$abu + pbv = b.$$

ab al divisible por p resulta que $abu + pbv$ se divide por p, es decir b admite p para divisor.□

TEOREMA 1.4. *Si el producto de muchos enteros se divide por un número primo p, entonces al menos uno de sus factores admite p para divisor*.

Demostración. (se efectúa por inducción sobre el número de los factores que se apoyan en el TEOREMA 1.3). Supóngase que el TEOREMA es verdadero para n factores. Sea $p \mid (a_1 \dots a_n)a_{n+1}$;por lo tanto, $p \mid (a_1 \dots a_n)a_{n+1}$. Según el TEOREMA 1.3, al menos uno de los dos números $a_1 \dots a_n$ y a_{n+1} se divide por p. Si a_{n+1} no se divide por p, el

producto $a_1 \dots a_n$, por lo contrario, se divide por p .Por consiguiente, según la hipótesis de inducción, al menos uno de los números $a_1 \dots a_n$ se divide por p . □

TEOREMA 1.5. *Todo entero positivo diferente de 1 puede representarse bajo la forma de producto de factores primos positivos. Esta representación es única al orden de los factores próximos.*

Demostración. Sea a un entero positivo diferente de 1. Demuéstrese la representatividad de a bajo la forma de producto de factores primos positivos al admitir que esta proposición es verdadera para todos los enteros positivos distintos de 1 e inferiores a a. Si a es primo, la proposición es verdadera. Si a es un número compuesto, se le puede representar bajo la forma de producto bc de enteros b, c inferiores a a y superiores a la unidad. Según la hipótesis de inducción, b y c pueden representarse bajo la forma de producto de factores primos positivos:

$$b = p_1 \dots p_r, \qquad c = p_{r+1} \dots p_m.$$

Al llevar estas factorizaciones en la igualdad $a = bc$, resulta la representación del número a

$$a = p_1 \dots p_r p_{r+1} \dots p_m$$

bajo la forma de un producto de factores primos positivos.

Demuéstrese la unicidad de esta representación al utilizar el método de inducción. Si a es primo, entonces la unicidad de la representación evidentemente se deriva de la definición del número primo. Supóngase que para todos los números inferiores a a la unicidad de la representación se respeta. a al suponerse compuesto, se consideran dos representaciones cualesquiera del número a bajo la forma de producto de factores primos positivos:

$$(1)\ a = p_1 \dots p_m = q_1 \dots q_n.$$

Dado que $p_1 | q_1 \dots q_n$, según el TEOREMA 1.4, al menos uno de los factores $q_1 \dots q_n$ es divisible por p; para una numeración adecuada, puede admitirse que $p_1 | q_1$. Puesto que p_1 y q_1 son factores primos positivos, resulta $p_1 = q_1$. Al simplificar los dos miembros de la igualdad (1) por p_1 y plantear $a/p1 = a_1$, se obtiene

$$a_1 = p_1 \dots p_m = q_2 \dots q_n.$$

Como el número a_1 es inferior a a, por hipótesis de inducción, a_1 posee una representación única bajo la forma de producto de factores primos positivos; por tanto, $m = n$ y, para una numeración adecuada, $p_2 = q_2, \dots, p_m = q_m$. El número a posee así una representación única bajo la forma de producto de factores primos positivos. □

COROLARIO 1.6. *Todo entero c diferente de cero y de* ± 1 *se representa de manera única bajo la forma de producto*

$$(1)\ c = \mathcal{E} p_1 \dots p_m,$$

donde $p_1 \dots p_m$ *son números primos positivos y* $\mathcal{E} = \pm 1$.

En la representación (1) pueden aparecer números primos idénticos. Si se juntan factores primos idénticos en la representación (1) y se modifica, si es necesario, la numeración, puede representarse (1) bajo la forma

$$(2)\ c = \mathcal{E} p_1^{\propto} 1 p_2^{\propto} 2 \dots p_s^{\propto} s,$$

donde $p_1, \dots, p_s$ son números primos distintos, $\mathcal{E} = \pm 1$ y $\propto_i > 0$ para $i = 1, 2, \dots, s$. La representación de un entero (diferente de cero) bajo la forma (2) se le denomina su *factorización canónica*.

Divisores de un número entero: al conocer la factorización canónica de un número natural, se está en la capacidad de describir los divisores de ese número.

PROPOSICIÓN 1.7. *Sea n un número natural y*

(1) $n = p_1^{\propto}1p_2^{\propto}2 \dots p_s^{\propto}s$

Su factorización canónica. Entonces cada divisor natural d del número n puede escribirse bajo la forma

(2) $d = p_1^{\delta}1p_2^{\delta}2 \dots p_s^{\delta}s$,

donde δ_i son enteros que satisfacen las condiciones

(3) $\delta_i \in \{0,1, \dots, \propto_i\}$ Para $i = 1,2, \dots, s$.

Demostración. sea d un divisor natural cualquiera del número n. Dado que cada divisor primo del número d es un divisor del número n, en la factorización de d, debido a (1), solo se puede encontrar números del conjunto $\{p_1, \dots, p_s\}$. También el δ_i número d puede representarse bajo la forma (2), los exponentes δ_i satisfacen las condiciones (3).

Por otra parte, si d adquiere la representación (2) y los exponentes δ_i satisfacen las condiciones (3), se obtiene

$n = d\left(p_1^{\propto 1-\delta 1} \dots p_s^{\propto s-\delta s}\right)$ $(\propto_i - \delta_i \geq 0)$,

es decir d es un divisor natural del número n.

Número y suma de divisores naturales de un número. La proposición 1.7 permite calcular el número y la suma de los divisores naturales de un número.

PROPOSICIÓN *1.8. Sea $n = p_1^{\propto 1} \dots p_s^{\propto}s$ la factorización canónica del número natural n. Entonces el número $\tau(n)$de los divisores naturales del número n se expresa por la formula $\tau(n) = (\propto_1 + 1) \dots (\propto_s + 1)$.*

Demostración. según la proposición 1.7, todo divisor natural d del número n puede representarse bajo la forma

$d = p_1^{\delta 1} \dots p_s^{\delta s}$,

donde

(3) $\delta_i \in \{0,1, \dots, \propto_i\}$ Para $i = 1,2, \dots, s$.

También para encontrar el número de todos los divisores naturales del número n basta calcular el número de todas las colecciones ordenadas $\delta_1, \dots \delta_s$ que satisface las condiciones (3). Como resultado de (3) δ_i puede adoptar $\propto_i + 1$ valores, las elecciones de los diferentes valores de $\delta_1, \dots \delta_s$ siendo independientes el uno del otro y, conforme a la unicidad de la factorización, en colecciones diferentes corresponden a n divisores distintos. Por consiguiente, el número de todos los divisores naturales del número n es $(\propto_1 + 1) \dots (\propto_s + 1)$.

Ejemplos. 1. Sea $n = 180. \text{Entonces}, 180 = 2^2.3^2.5$ y

$\tau(180) = (2+1)(2+1)(1+1) = 18.$

2. sea $n = 60. \text{Entonces}, 60 = 2^2.3.5$ y

$\tau(60) = (2+1)(1+1)(1+1) = 12.$

Proposición.1.9. Sea $n = p_1^{\propto 1} \dots p_s^{\propto s}$ *la factorización canónica del número natural* n. *La suma* $\sigma\,(n)$*de todos los divisores naturales del número* n *entonces se expresa por la fórmula*

(4) $\sigma\,(n) = \frac{p_1^{\propto 1}-1}{p_1-1} \dots \frac{p_s^{\propto s}-1}{p_s-1}$.

Demostración. según la proposición 1.7, cada divisor del número n adopta la forma
$p_1^{\delta 1} \dots p_s^{\delta s}$ y

(5) $\sigma\,(n) = \sum_{\substack{p_1^{\delta 1}\dots p_s^{\delta s}. \\ \delta 1 \in \{0,1,\dots,\propto_1\} \\ \dots\dots\dots \\ \delta s \in \{0,1,\dots,\propto_2\}}}$

Se ve fácilmente que cada término de la suma en (5) se encuentra exactamente una vez después de la eliminación de paréntesis del producto

(6) $(1 + p_1 + \dots + p_1^{\propto 1}) \dots (1 + p_s + \dots + p_s^{\propto s})$.

Por lo tanto, la suma es igual al producto (6). Cada factor al ser una suma de términos de una progresión geométrica, el producto

(6) es

$$\frac{p_1^{\propto 1+1}-1}{p_1-1} \dots \frac{p_s^{\propto s+1}-1}{p_s-1}.$$

La fórmula (4) se verifica. □

Ejemplo: sea $n = 60$. Entonces $n = 2^2 \cdot 3 \cdot 5$ y

$$\sigma\,(60) = \frac{2^3-1}{2-1}.\frac{3^2-1}{3-1}.\frac{5^2-1}{5-1} = 7.4.6 = 168.$$

Conjunto infinito de números primos: Euclides demostró el siguiente TEOREMA.

TEOREMA 1.10. *Un conjunto de números primos positivos es infinito*.

Demostración. Muéstrese que para cada conjunto finito dado de números primos positivos $p_1, \dots, pn$ existe un número primo positivo diferente de todos los números de este conjunto. Para tal fin, considérese el número

$$a = p_1.p_2 \dots p_n + 1.$$

a al ser un número natural superior a la unidad, según el TEOREMA 1.5, se puede descomponer en un producto de factores primos positivos y, de hecho, tiene al menos un divisor primo positivo p. Este divisor difiere de $p_1.p_2, \dots, p_n, = 1$, ya que, en el caso contrario $p|p_1 \dots p_n$, $p|a$ y la diferencia $a = p_1.p_2 \dots p_n = 1$ se dividiría por p, sin embargo, es imposible. Por consiguiente, el conjunto de todos los primos es infinito. □

Criba de Eratóstenes: Analícese el método de obtención de primos positivos no superior a un número dado.

PROPOSICIÓN 1.11. *Un número compuesto positivo* a *posee al menos un divisor primo positivo no superior a* $\sqrt{a}$.

Demostración. entre los divisores positivos del número a diferentes de la unidad existe un menor; denótese por p. Si el número p fuese compuesto, tendría un divisor positivo q que satisface las condiciones $1 < q < p$. En este caso el número q seria un divisor positivo del número a inferior a p, lo que es una contradicción con la selección del número p.

Puesto que, p es un número primo. Si $a = pb$, entonces $b \geq p$. Al multiplicar miembro a miembro $a = pb$ y $b \geq p$ y al simplificar por b, se obtiene $a \geq p^2$ y $p \leq \sqrt{a}$.

PROPOSICIÓN 1.12. *Si un número positivo a diferente de la unidad no se divide por ningún número primo positivo no superior a $\sqrt{a}$, entonces es primo.*

Esta proposición se deriva directamente de la proposición 1.11, existe un método sencillo de construcción de tabla de números primos positivos no superior a un entero dado. A este método se le denomina *criba de Eratóstenes*.

Supóngase que se trata de encontrar todos los números positivos no superior a un número natural a. Para ello, se escribe la sucesión de todos los números naturales de 2 a a: $2, 3, 4, \ldots, a$. En esta sucesión colóquese el segundo número después de 2. El primer número no eliminado es el número 3. Luego, se tacha cada tercer número después de tres (cuenta los números ya tachados). El siguiente número primo no tachado seguido de 3 es el número primo 5. Elimínese cada quinto número después de 5, etc. Se continuará esta eliminación hasta que se alcance el primer número primo no inferior a $\sqrt{a}$. Conforme a la proposición 1.12, todos los números no tachados serán primos positivos no superior a a.

Ejemplo: Constrúyase la tabla de primos positivos no superior a 50. Para ello, escríbase los números naturales del 2 al 50 y se procede a las eliminaciones hasta encontrar el número primo superior o igual a $\sqrt{50}$, es decir hasta 11 (los números tachados están en negrita):

2 **3** 4 **5** 6 **7** 8 **9** 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20 21 22 **23** 24 25 26 27 28 **29** 30 **31** 32 33 34 35 36 **37** 38 39 40 **41** 42 **43** 44 45 46 **47** 48 49 50

Elimínese esta sucesión en cada segundo número después de 2, luego cada tercer después de 3, después cada quinto número después de 5 y, al finalizar, cada séptimo después del número 7. Todos los números restantes serán primos. Así se obtiene la tabla siguiente de la sucesión de números primos positivos inferiores a 50:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Ejercicios

1. Mostrar que para todo entero n el número $n\ (n+1)(n+2)$ es divisible por 6.
2. Mostrar que para todo entero n el número $n\ (n+1)(2n+1)$ es divisible por 6.
3. Sea m y n enteros primos entre sí. Demostrar que son primos entre si los números siguientes: m y $m+n$, m y $m-n$, $m+n$ y $2m+n$.
4. Sean a, b, c, d enteros positivos y a/b, c/d fracciones irreducibles. Demostrar que si a/b=c/d, entonces $a = c$ y $b = d$.
5. Mostrar que si $2^n + 1$ es un número primo, entonces $n = 2^m$.
6. Mostrar que si $2^n - 1$ es un número primo, entonces n es primo.
7. Sean a y n enteros positivos, $a > 1$. Demostrar que si $a^n + 1$ es un número primo, entonces $n = 2^m$.
8. Factorizar el número 50!
9. Mostrar que con un número natural $n > 1$ la suma $1 + \frac{1}{2} + \cdots + \frac{1}{n}$ no puede ser un número entero.
10. Un número natural es denominado perfecto si es igual a la mitad de la suma de sus divisores positivos. Demostrar que todo número par perfecto es de la forma $2^n(2^{n+1} - 1)$, donde $n \in \boldsymbol{N}$, con $2^{n+1} - 1$ primo.

§2. Máximo común divisor y mínimo común múltiplo.

Máximo común divisor: un entero c se le denomina *divisor común de enteros* $a_1, \dots, a_n$ si c divide cada uno de los números.

DEFINICIÓN: se le denomina *máximo común divisor de enteros* $a_1, \dots, a_n$ un común divisor divisible por todo común divisor de estos números. De enteros $a_1, \dots, a_n$ se le denomina *primos entre sí,* si su máximo común divisor es la unidad.

Un máximo común divisor de números $a_1, \dots, a_n$ se denota: MCD $(a_1, \dots, a_n)$; un máximo común divisor positivo de estos números se denota MCD $(a_1, \dots, a_n)$.

COROLARIO 2.1. *Si d es un máximo común divisor de enteros $a_1, \dots, a_n$, el conjunto de todos los divisores comunes de estos números coinciden entonces con el conjunto de todos los divisores del número d.*

COROLARIO 2.2. *Dos cualesquiera máximo comunes divisores de enteros $a_1, \dots, a_n$ están asociados, es decir solo difieren del signo. Si d es un máximo común divisor de números $a_1, \dots, a_n$, entonces el número $(-d)$ es igualmente un máximo común divisor de estos números*.

PROPOSICIÓN 2.3. Si $a = \prod_{p|a} p^{\propto p}$ y $b = \prod_{p|b} p^{\beta p}$ *son factorizaciones canónicas de enteros positivos a y b, el número*

$$d = \prod_{\substack{p|a \\ p|b}} p^{\min\ (\alpha p, \beta p)}$$

es entonces el máximo común divisor de números a y b.

Demostración. el número d es un divisor de a como de b conforme a la proposición 1.7, dicho de otra manera, d es el común divisor de a y b. Luego, si c es un común divisor cualquiera positivo de a y b, conforme a la proposición 1.7,

$$c = \prod_{\substack{p|a \\ p|b}} p^{\Upsilon p,}$$

en particular, para cada divisor de a y b, se obtiene las desigualdades $\Upsilon_p \leq \alpha_p$, $\Upsilon_p \leq \beta_p$. Por lo tanto, $c|d$. Por consiguiente, d es un máximo común divisor de números a y b.□

Sean $a_1, \dots, a_n$ enteros cualquieras. Considérese el conjunto

(1) $I = \{k_1 a_1 + \cdots + k_n a_n | k_1, \dots, k_n \in \boldsymbol{Z}\}$

de todas las combinaciones lineales enteras de números $a_1, \dots, a_n$. Se verifica fácilmente que este conjunto es un ideal del anillo $\mathcal{Z}$. Este ideal se le denomina *ideal generado por los números* $a_1, \dots, a_n$ y se denota $(a_1, \dots, a_n)$.

TEOREMA 2.4. *Para toda colección de enteros $a_1, \dots, a_n$ existe un máximo común divisor. El número d es un máximo común divisor de números $a_1, \dots, a_n$ si y sólo si el ideal $(a_1, \dots, a_n)$ es igual al ideal (d).*

Demostración. si todos los números $a_1, \dots, a_n$ son iguales a cero, el único máximo común divisor de estos números es el número cero.

Demostración. si todos los números $a_1, \dots, a_n$son iguales a cero, el único máximo común divisor de estos números es el cero.

Supóngase que al menos uno de los números $a_1, \dots, a_n$ es diferente de cero. Considérese el conjunto I de todas las combinaciones lineales enteras de números $a_1, \dots, a_n$. El conjunto I contiene los números $a_s, s = 1, \dots, n$, puesto que

$a_s = k_1a_1 + \cdots + k_na_n$, donde $k_s = 1$ y $k_i = 0$ para $i \neq s$. por lo tanto, el conjunto I contiene los números diferentes de cero. El conjunto I es ideal del anillo de enteros generados por los números $a_1, \ldots, a_n$;$I = (a_1, \ldots, a_n)$. Según el TEOREMA 4.4, cada ideal del anillo $\mathbb{Z}$ es principal y, por consiguiente, se compone de múltiplos de algún número entero d, $I = dZ$. Demuéstrese que d es MCD $(a_1, \ldots, a_n)$. Como cada elemento del conjunto I es divisible por d, se obtiene $d|a_i$ para $i = 1, \ldots, n$, es decir que d es un divisor común de números $a_1, \ldots, a_n$. Luego, como $d \in I$, según (1), existe enteros $k_1, \ldots, k_n$ tales que

$$d = k_1a_1 + \cdots + k_na_n.$$

Resulta que todo divisor común c de los números $a_1, \ldots, a_n$ es igualmente un divisor del número nd. Así, todo elemento d al generar el ideal $I = (a_1, \ldots, a_n)$ es un máximo común divisor de los números $I = (a_1, \ldots, a_n)$. Resulta, en particular de la demostración, que toda colección finita de los números $a_1, \ldots, a_n$ posee un máximo común divisor.

Sea d' un máximo común divisor arbitrario de los números $a_1, \ldots, a_n$ y d, como siempre, un número que genera el ideal I; demuéstrese que $(a_1, \ldots, a_n) = (d')$. Todos MCD de los números $a_1, \ldots, a_n$ están asociados, es decir solo es diferente por el signo. Como resultado, $d' = \pm d$. Por lo tanto el ideal (d') coincide con el ideal (d). Por consiguiente, $(a_1, \ldots, a_n) = (d')$.□

El análisis de la demostración del TEOREMA anterior permite igualmente formular el TEOREMA siguiente.

TEOREMA 2.5. *Represéntese el máximo común divisor d de los enteros $a_1, \ldots, a_n$ bajo la forma de una combinación lineal entera de estos números, es decir bajo la forma $d = k_1a_1 + \cdots + k_na_n$ a los enteros $k_1, \ldots, k_n$. Esto, si los números $a_1, \ldots, a_n$ no son todos nulos, entonces $|d|$ es el menor entero positivo representable en esta forma. Todos los números representados en esta forma, dicho de otra forma, todos los números del ideal $(a_1, \ldots, a_n)$ son múltiplos del número d.*

PROPOSICIÓN 2.6. *Si un divisor común d de enteros $a_1, \ldots, a_n$ se representa bajo la forma de una combinación lineal entera de los números, d es entonces un máximo común divisor de números $a_1, \ldots, a_n$.*

Demostración. Supóngase que el divisor común d de los números $a_1, \ldots, a_n$ se representa bajo la forma

$$d = k_1a_1 + \cdots + k_na_n ,$$

donde $k_1, \ldots, k_n$ son enteros. En este caso todo divisor común de los números $a_1, \ldots, a_n$ divide la suma $k_1a_1 + \cdots + k_na_n$ y, que parte de d. Por lo tanto d es el máximo común divisor de los números $a_1, \ldots, a_n$.□

PROPOSICIÓN 2.7. Para todos los enteros a, b, c

MCD $(a, b, c) \sim$ MCD (MCD $(a, b), c$).

Demostración. Sea d_1, MCD (a, b) y d, MCD (d_1, c). Entonces d es divisor común de números d_1 y c , mientras que el número d_1 es un divisor común de números a y b. Por lo tanto, d es un divisor de los números a, b y c. Según el TEOREMA 2.5, los números d y d_1 pueden representarse bajo esta forma

$$d = kd_1 + k_3c, \qquad d_1 = k_1a + k_2b,$$

donde k, k_1, k_2, k_3 son enteros; también se obtiene $d = kk_1a + kk_2b + kk_3c$. Así, el divisor común d de los números a, b, c pueden expresarse linealmente en el medio de los números. Por consiguiente, según la proposición 2.6, d es el máximo común divisor de estos números. □

Esta proposición permite reducir la búsqueda del máximo común divisor de muchos números al buscar el máximo común divisor de dos números.

PROPOSICIÓN 2.8. Para enteros cualquieras a, b y c

MCD $(ac, bc) \sim c$. MCD (a, b).

Demostración. Sea d un MCD (a, b). Entonces, según el TEOREMA 2.5, d puede representarse bajo la forma

$$d = k_1 a + k_2 b,$$

donde k_1 yk_2 son enteros, por lo tanto $cd = k_1 ac + k_2 bc$. Así mismo, como d es el divisor común de a y b, cd es de ac y bc. Por consiguiente, según la proposición 2.6, el número cd es un máximo común divisor de ac y bc. □

Números primos entre sí: Analícese las propiedades de los números primos entre sí.

PROPOSICIÓN 2.9. *Los números enteros $a_1, \dots, a_n$ son primos entre sí, sí y sólo si la unidad se representa bajo la forma de una combinación lineal entera de estos números.*

Demostración. Si los números $a_1, \dots, a_n$ son primos entre sí, su máximo común divisor, la unidad, se representa, según el TEOREMA 2.5, bajo la forma de una combinación lineal entera de estos números.

Recíprocamente, si la unidad se representa bajo la forma de una combinación lineal entera de los números $a_1, \dots, a_n$, entonces, conforme a la proposición 2.6, la unidad es un máximo común divisor de los números. Por lo tanto, los números $a_1, \dots, a_n$ son primos entre si.□

PROPOSICIÓN 2.10. *Los enteros $a_1, \dots, a_n$ son primos entre sí, sí y sólo si no poseen divisor primo común.*

La demostración se deja en manos del lector.

TEOREMA 2.11. *Si un número entero divide el producto de dos enteros y es primo con uno de los factores, entonces el divide al otro factor*.

Demostración. Sea a y b dos primos entre si y a divide a bc. Demuéstrese que a divide c. a y b siendo primos entre sí, existe enteros k_1 y k_2, tales que

$$k_1 a + k_2 b = 1.$$

Al multiplicar los dos miembros de la igualdad por c, se cumple $k_1 ac + k_2 bc = c$. Además a divide bc. Por lo tanto, a divide $k_1 ac + k_2 bc$, es decir a divide c.□

PROPOSICIÓN 2.12. *Un divisor común d de los enteros $a_1, \dots, a_n$ no simultáneamente nulos es su máximo común divisor si y sólo si $a_1/d, \dots, a_n/d$ son primos entre sí.*

Demostración. Dado que por hipótesis los números $a_1, \dots, a_n$ no todos son nulos, se obtiene $d \neq 0$. Si d es el máximo común divisor de los números $a_1, \dots, a_n$, entonces, según el TEOREMA 2.5, puede expresarse linealmente mediante $a_1, \dots, a_n$:

(1) $k_1 a_1 + \cdots + k_n a_n = d,$

donde $k_1, \dots, k_n$ son enteros. Al dividirse los dos miembros de la igualdad por d, se cumple

(2) $k_1 \frac{a_1}{d} + \cdots + k_n \frac{a_n}{d} = 1.$

De ahí, según la proposición 2.9, se deduce que los números $a_1/d, \dots, a_n/d$ son primos entre sí.

Recíprocamente: si los números $a_1/d, \dots, a_n/d$ son primos entre sí, entonces, según la proposición 2.9, existen enteros $k_1, \dots, k_n$ los cuales satisfacen la igualdad (2). Al multiplicar los dos miembros de esta igualdad por d, se obtiene la igualdad (1). Dado que el divisor común d de los números $a_1, \dots, a_n$ se representa bajo la forma de una combinación lineal de estos números, según la proposición 2.6, el número d es un máximo común divisor de $a_1, \dots, a_n$.□

Mínimo común múltiplo. El entero c se le denomina *múltiplo común de los enteros* $a_1, \dots, a_n$ si es divisible por cada uno de estos números.

DEFINICIÓN: se le denomina *mínimo común múltiplo de los enteros* $a_1, \dots, a_n$ un tal múltiplo común que divide todo múltiplo común de estos números. Un mínimo común múltiplo de los enteros $a_1, \dots, a_n$ se denota MCM $(a_1, \dots, a_n)$. Un mínimo común múltiplo positivo de los números $a_1, \dots, a_n$ diferentes de cero se denota $[a_1, \dots, a_n]$.

De la definición del MCM $(a_1, \dots, a_n)$ se extrae directamente el corolario.

COROLARIO 2.13. *Dos mínimos comunes múltiplos cualesquiera de los números* $a_1, \dots, a_n$ *están asociados en* $\mathcal{Z}$*, es decir solo difiere del signo. Si* m *es MCM* $(a_1, \dots, a_n)$*, el número* $(-m)$ *es por lo tanto MCM* $(a_1, \dots, a_n)$.

COROLARIO 2.14. *Si* m *es un mínimo común múltiplo de los números* $a_1, \dots, a_n$ *, entonces el conjunto de todos los múltiplos comunes de estos números coinciden con el conjunto de todos los múltiplos del número* m.

PROPOSICIÓN *2.15. Sea* $a = p_1^{\propto 1} \dots p_s^{\propto} s$ *y* $n = p_1^{\beta 1} \dots p_s^{\beta} s$*, donde* $p_1, \dots, p_s$ *son números positivos diferentes de dos a dos primos entre si y* $\propto_i, \beta_i$*de los enteros no negativos. Entonces*
$[a, b] = P^{max(\propto_i, \beta_i)} \dots P_S^{max(\propto_s, \beta_s)}$.

La demostración de esta proposición se deja a manos del lector.

TEOREMA 2.16. *Para toda colección de enteros* $a_1, \dots, a_n$ *existe un mínimo común múltiplo. El entero* m *es MCM* $(a_1, \dots, a_n)$*, si y solo si* $(a_1) \bigcap \dots \bigcap (a_n) = (m)$*, donde* (a_i) *es el ideal generado por el número* a_i.

Demostración. Considérese el conjunto

(1) $I = (a_1) \bigcap \dots \bigcap (a_n)$.

Dado que los conjuntos $(a_1) \dots (a_n)$ son cerrados con respecto a la adición y a la multiplicación por enteros, se verifica fácilmente que su intersección I es igualmente cerrada con respecto a la adición y a la multiplicación por enteros. Así mismo, este conjunto no es vacio, puesto que contiene un cero. Por consiguiente, I es un ideal del anillo de enteros. Según el TEOREMA 4.4, todo ideal del anillo de enteros es principal, es decir existe un entero m, tal que cada número de I sea múltiplo de m, $I = (m)$. Se demuestra que m es *MCM* $(a_1, \dots, a_n)$. Como $m \in I$, entonces, según (1), $m \in (ai)$ para $i = 1, \dots, m$, es decir m es un mínimo común múltiplo de los números $a_1, \dots, a_n$. Además m' es un múltiplo común cualquiera de los números $a_1, \dots, a_n$ se obtiene entonces $m' \in (a_1) \dots m' \in (a_n)$. por consiguiente, $m' \in I = (a_1) \bigcap \dots \bigcap (a_m) = (m)$ y, por consiguiente m' es divisible por m. Así, m es un mínimo común múltiplo de los números $a_1, \dots, a_n$.

Ahora supóngase que m_1 es un mínimo común múltiplo de los números $a_1, \dots, a_n$ y demuéstrese que $m_1 = (a_1) \bigcap \dots \bigcap (a_n)$. Como los números m_1 y m son mínimos comunes múltiplos de una misma colección de números $a_1, \dots, a_n$, por lo tanto están asociados en $\mathbb{Z}$, es decir $m_1 = \pm m$. Por consiguiente, $m_1 = m$ y por lo tanto, $(a_1) \bigcap \dots \bigcap (a_n) = (m_1)$.□

PROPOSICIÓN 2.17. *Para los enteros* $a, b,$ *y* c *diferentes de cero con* $c > 0$*, se obtiene:* $[ac, bc] = c[a, b]$.

Demostración. Sea $m = [a, b]$. Dado que m es un múltiplo común de a y b, cm es un múltiplo común de los números ac y bc. Sea m' un múltiplo común cualquiera de los números ac y bc, es decir

$m' = kac = sbc$,

donde k y s son enteros. Como $c \neq 0. ka = sb$. Por lo tanto, ka es divisible por m y, por lo tanto, m' es divisible por mc. Así, cm es un mínimo común múltiplo de los números ac y bc. Así mismo, $cm > 0$; por lo tanto$[ac, bc] = cm = c[a, b]$.□

COROLARIO 2.18. *Para todos los enteros* a, b *y* c *diferentes de cero* MCM $(ac, bc) \sim c. MCM\ (a, b)$.

PROPOSICIÓN 2.19. *Si los enteros a y b son primos entre sí, ab entonces es un mínimo común múltiplo de los números a y b.*

Demostración. El número ab es un múltiplo común de a y *de* b.por lo tanto, basta demostrar que todo múltiplo común m de los números a *y* b es divisible por ab. El número m es múltiplo de b, es decir $m = bc$, *donde* c es un entero, y $a|bc$. Como, por hipótesis, a *y* b son primos entre si se deduce, según el TEOREMA 2.11, que a divide c, $c = ad$. Por consiguiente, $m = abd$, es decir m es divisible por ab. Así, ab es un mínimo común múltiplo de los números a *y* b.□

PROPOSICIÓN 2.20. *Si los enteros a y b son diferentes de cero, se obtiene*

(1) MCM $(a, b) \sim |\frac{ab}{PGCD(a,b)}$.

Demostración. Sea d un máximo común divisor de los números a y b. a y b *que sean diferentes de cero*, tenemos $d \neq 0$. según el corolario 2.18,

(2) MCM $(a, b) \sim d$ MCM $(a/d\,, b/d)$.

Luego, en virtud de la proposición 2.12, Máximo Común Divisor$(a/d\,, b/d) = 1$.
De donde, en razón de la proposición 2.19,

(3) MCM $\left(\frac{a}{d}\,, \frac{b}{d}\right) \sim \frac{a}{d}\,.\frac{b}{d}$.

Sobre la base de (2) y (3) concluimos que la relación (1) se verifica. □

TEOREMA 2.21. *Para todos los enteros a, b* y c, tenemos

(1) MCM $(a, b, c) \sim$MCM (MCM$(a, b), c)$.

Demostración. Sea $m =$ el Mínimo Común Múltiplo $(a, b, c), m_1 =$ Máximo Común Múltiplo (a, b) y $m' =$ Máximo Común Múltiplo (m_1, c). Según el TEOREMA 2.16, se tiene

(2) $(m) - (a) \cap (b) \cap (c) \quad (m_1) = (a) \cap (b).\ \left(m'\right) = (m_1) \cap (c)$.

Por tanto

(3) $\left(m'\right) = ((a) \cap (c) = (a) \cap (b) \cap (c)$.

De (2) Y (3) se deduce que $(m) = \left(m'\right)$. □

Ejercicios

1. Sean a y b enteros positivos primos entre ellos. Mostrar que la suma $\frac{1}{a}+\frac{1}{a+b}$después reducción al mismo denominador es una fracción irreductible.
2. Demostrar que d es el máximo común divisor de los enteros a, b, c si y si solo si $a/d\,, b/d\,, c\,/\,d$ son los primos enteros entre ellos.
3. Demostrar que para todo enteros cualquiera a, b, c, k Máximo Común Divisor $(ka, kb, kc)\sim k$ Máximo Común Divisor (a, b, c).
4. Demostrar que el común múltiplo m de los enteros a, b, c es un mínimo común múltiplo si y solo si los números $m/a\,, m/b\,, m\,/\,c$ son primos entre ellos $(a, b, c\ \neq 0)$.
5. Sea $a = m/n$, donde m, n son los primos enteros entre ellos, $m \neq 0$ y $n > 0$. Si $a = r/s$, donde r, s son los enteros y $s > 0$, entonces existe un numero natural t, tal que $r = tm$ y $s = tn$. Además, t es un máximo común divisor de los números r y s.

§3. Algoritmo de Euclides y fracciones continúas finitas

Algoritmo de Euclides. Estúdiese el más simple proceso de obtención del máximo común divisor de dos enteros.
PROPOSICIÓN 3.1. *Sean a y b dos enteros*, $b \neq 0$ y

$$(1) a = bq + r \qquad (0 \leq r < |b|).$$

Entonces máximo común divisor(a, b) =máximo común divisor(b, r).

Demostración. Se deduce que(1) todo común divisor de números a y b es un divisor de número $r = a - bq$ y que todo común divisor de números b y r es un divisor de números a. El conjunto de todos los comunes divisor de los números a y b coincide por tanto con el conjunto de todos los comunes divisor de los números b y r. se deduce que el común divisor positivo de los números a y b coincide con el común divisor positivo de los números b y r, es decir máximo común divisor(a, b) =máximo común divisor(b, r). □

Si $b|a$, donde $b \geq 1$, es evidente que máximo común divisor$(a, b) = b$. para encontrar el máximo común divisor de dos números enteros usaremos el proceso de *división sucesiva* denominado *algoritmo de Euclides*. El principio de este proceso reside en el hecho que en virtud de la proposición demostrada anteriormente el problema de la búsqueda de máximo común divisor de los números de a y b se reduce a un problema más simple de la búsqueda de máximo común divisor de b y r, donde $0 \leq r\ < |b|$. Si, en cambio,$r \neq 0$, retomasmos el razonamiento a partir de b y r. Finalmente, se obtiene
una serie de igualdades

$$\begin{aligned}
&a = ba_0 + r_1, && 0 < r_1 < |b|,\\
&b = r_1a_1 + r_2, && 0 < r_2 < r_1,\\
&(2)\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\\
&r_{n-2} = r_{n-1}a_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
&r_{n-1} = r_na_n + r_{n+1}.
\end{aligned}$$

Se obtiene una serie decreciente de los números naturales

$$r_1 > r_2 > \cdots > r_n > \cdots \geq 0,$$

que no puede ser infinita. Existe por tanto un resto igual a cero; sea $r_{n+1} = 0, r_n \neq 0$.

Sobre la base de la proposición 3.1 a partir de la igualdad (2) tenemos máximo común divisor$(a, b) =$ máximo común divisor(b, r_1) =máximo común divisor$(r_1, r_2) = \cdots =$ máximo común divisor$(r_{n-1}, r_n) =$ máximo común divisor$(r_n, 0) = r_n$,
es decir r_n =máximo común divisor(a, b). En resumen, se llega a la deducción: si en los enteros a, b, donde $b \neq 0$, se aplica el algoritmo de Euclides, entonces el último residuo no nulo de este algoritmo es máximo común divisor(a, b).

Fracciones continúas finitas. Cualquier número racional se puede representar bajo la forma de a/b, donde a y b son enteros y b≥ 1.
Al aplicar a a y b al algoritmo de Euclides, se obtiene una serie de igualdades:

$$a = ba_0 + r_1,$$
$$b = r_1a_1 + r_2,$$
$$r_1 = r_2a_2 + r_3,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$r_{n-3} = r_{n-2}a_{n-2} + r_{n-1},$$
$$r_{n-2} = r_{n-1}a_{n-1} + r_n,$$
$$r_{n-1} = r_na_n,$$

donde $b > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$. Esta serie de igualdades puede escribirse bajo la forma

$$\frac{a}{b} = a_0 + \frac{r_1}{b},$$
$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1},$$
$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2},$$
$$\cdots\cdots\cdots\cdots$$
$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}},$$
$$\frac{r_{n-1}}{r_n} = a_n.$$

Sirviéndose de estas igualdades, es posible de explicar $a\ /\ b$ por medio de los números $a_0, a_1, \cdots, a_n$. En efecto, la primera igualdad puede escribirse bajo la forma

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}};$$

que sustrae en $b\ /\ r_1$su expresión obtenida de la segunda igualdad,
resulta

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}},$$

etc. Finalmente, se obtiene

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

La expresión que se encuentra en el segundo miembro de esta igualdad se denomina *fracción continua*.

DEFINICIÓN. Se *llama fracción continua finita* a la expresión de la forma

$$(1)\ \ a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}},$$

donde a_0 es un entero, $a_1, \cdots, a_n$de los enteros positivos y $a_n > 1$.

Usualmente, una fracción continua (1) se escribe de manera abreviada de este modo:

$$|a_0; a_1, a_2, \cdots, a_n|.$$

Los razonamientos presentados anteriormente muestran que todo número racional se puede representar bajo la forma de una fracción continua finita.

Ejemplo. Desarróllese en fracción continua el número $\frac{126}{37}$.

Con la ayuda del algoritmo de Euclides obtenemos:

$$\frac{126}{37} = +\frac{15}{37} = 3 + \frac{1}{\frac{37}{15}} = 3 + \frac{1}{2 + \frac{1}{\frac{15}{7}}} = 3 + \frac{1}{2 + \frac{1}{2\frac{1}{7}}}$$

o

$$\frac{126}{37} = |3; 2,2,7| \cdot$$

Se puede mostrar que todo número racional posee una única representación bajo la forma de fracción continua finita.

Reducidas. Sea

$$(1) a_0 + \cfrac{1}{a_1 + \ddots} = |a_0; a_1, \cdots, a_n|$$

una fracción continúa finita. La fracción continúa

$$(2)\ A_k = |a_0; a_1, \cdots, a_k|,$$

donde $k \in \{0,1 \cdots, n\}$, se denomina *k-ésima reducida* de la fracción (1).

Por definición, *la reducida nula* de la fracción (1) es el número $A_0 == a_0$. Nótese que la $(K+1)$-ésima reducida A_{k+1} puede ser obtenida a partir de la K-ésima reducida A_k por sustitución en el elemento a_k del elemento $a_k + \frac{1}{a_{k+1}}$.

Defínase los números P_k y $Q_k (K \in \{0,1 \cdots, n\})$por recurrencia por medio de las fórmulas siguientes:

$P_0 = a_0,$ $\qquad Q_0 = 1,$

$P_1 = a_0 a_1 + 1,$ $\qquad Q_1 = a_1,$

. . . . $\qquad$ . . . . .

$P_k = P_{k-1} a_k + P_{k-2}, Q_k = Q_{k-1} a_k + Q_{k-2}$

$(K \in \{2,3, \cdots, n\}).$

TEOREMA 3.2. *Para toda reducción A_k de la fracción continua* (1). Se tiene la igualdad

$(4) A_k = \frac{P_k}{Q_k} (K = 0,1,\cdots,n).$

Demostración. La fórmula(4) se demuestra por recurrencia en k. A partir de la fórmula (3) resulta directamente de las igualdades

$$A_0 = \frac{a_0}{1} = \frac{P_0}{Q_0},$$

$$A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_0 + 1}{a_1} = \frac{P_1}{Q_1},$$

es decir que la afirmación del TEOREMA se verifica para $k = 0$ y $k = 1$. Así que,

$$A_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{(a_0 a_1 +) a_2 + a_0}{a_1 a_2 + 1} = \frac{P_1 a_2 + P_0}{Q_1 a_2 + Q_0}$$

significa que la afirmación del TEOREMA se comprueba para $k = 2$.

Supóngase que la afirmación del TEOREMA es verdadera para la m-ésima reducida, donde $2 \leq m < n$, es decir

$(5)\ A_m = \frac{P_m}{Q_m},$

y demuéstrese que la afirmación del TEOREMA se comprueba para $(m+1)$-ésima reducida. Sobre la base de las fórmulas (3) la igualdad (5) se puede escribir bajo la forma

$(6)\ A_m = \frac{P_{m-1} a_m + P_{m-2}}{Q_{m-1} a_m + Q_{m-2}}.$

Sustitúyase en los dos miembros de la igualdad (6) en el elemento a_m el elemento $a_m + \frac{1}{a_{m+1}}$. Esta sustitución transforma A_m en A_{m+1} y, como resultado, se obtiene a partir de (6)

$$A_{m+1} = \frac{P_{m-1}\left(a_m + \frac{1}{a_{m+1}}\right) + P_{m-2}}{Q_{m-1}\left(a_m + \frac{1}{a_{m+1}}\right) + Q_{m-2}} = \frac{(P_{m-1} a_m + P_{m-2}) a_{m+1} + P_{m-1}}{(Q_{m-1} a_m + Q_{m-2}) a_{m+1} + Q_{m-1}}.$$

De ahí, conforme a (3),

$$A_{m+1} = \frac{P_m a_{m+1} + P_{m-1}}{Q_m a_{m+1} + Q_{m-1}} = \frac{P_{m+1}}{Q_{m+1}}.$$

Así, la verdad de la fórmula (4), para $k = m$, resulta de la verdad de esta fórmula para $k = m + 1$. así pues la fórmula (4) es verdadera para cualquiera $k \in \{0,1,\cdots,n\}$.

Los números P_k y $Q_k$definidos para las fórmulas (3) respectivamente llamados *numerador* y *denominador de la k-ésima reducida*. Las fórmulas (3) proporcionan un método cómodo cálculo sucesivo de numeradores P_k y de denominadores Q_k reducidos. El cálculo se simplifica si cumple el siguiente esquema:

a_k		a_0	a_1	a_2	a_3	$\cdots$	a_n
P_k	1	a_0	P_1	P_2	P_3	$\cdots$	P_n
Q_k	0	1	Q_1	Q_2	Q_3	$\cdots$	Q_n

Ejemplo. Busquemos los reducidos de la fracción continua$|2; 5,7,3|$:

a_k		2	5	7	3
P_k	1	2	11	79	248
Q_k	0	1	5	36	113

Así, los reducidos de la fracción continua $|2; 5,7,3|$son las fracciones

$$A_0 = \frac{P_0}{Q_0} = \frac{2}{1}, A_1 = \frac{P_1}{Q_1} = \frac{11}{5},$$

$$A_2 = \frac{P_2}{Q_2} = \frac{79}{36}, \quad A_3 = \frac{P_3}{Q_3} = \frac{248}{113}.$$

TEOREMA 3.3. *Para $k \in \{1, \cdots, n\}$ se cumple la igualdad*

$$(7) P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k.$$

Demostración. Sea $\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k$.
Sobre la base de las fórmulas (3) la igualdad (7) se comprueba para $k = 1$:

$$(8)\ \Delta_1 = P_0Q_1 - Q_0P_1 = a_0a_1 - 1(a_0a_1 +) = -1.$$

Además, según (3),

$$\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k = P_{k-1}(Q_{k-1}a_k + Q_{k-2}) -$$

$$-Q_{k-1}(P_{k-1}a_k + P_{k-2}) = P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2} = -\Delta_{k-1}$$

$$(k \in \{2, \cdots, n\}).$$

Conforme a (8), se deduce que

$\Delta_k = (-1)^k$para $k \in \{1,2, \cdots, n\}$,

en otras palabras, la igualdad (7) se comprueba. □

COROLARIO 3.4. Los números P_k y $Q_k$son los primos entre ellos y, como serie de cada fracción P_k / Q_k es irreductible.

Demostración. Debido a (7) cualquier factor común de P_k y Q_k es divisor de la unidad. Así pues, los números P_k, Q_k son los primeros entre ellos y la fracción P_k / Q_k es intratable.□

Existe entre dos reducidos sucesivos una relación importante que deriva de (7)-

COROLARIO 3.5. Para $k \in \{1, \cdots, n\}$se comprueba la igualdad

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_{k-1}Q_k}.$$

Ejercicios

1. Sirviéndose del algoritmo de Euclides buscar:
   a) Máximo Común Divisor (549,387); b) Máximo Común Divisor (589,343); c) Máximo Común Divisor (12 606,64 994).

2. Desarrollar en fracción continua las fracciones ordinarias siguientes:

a) 2,3547, b) $\frac{99}{170}$.

3. simplificar utilizando el desarrollo en fracción continua $\propto = \frac{7857}{9153}$.

4. Se sabe que $3{,}141592653 < \pi < 3{,}141592654$, buscar los cuatros primos reducidos para el número π.

5. se sabe que $e = 2{,}71828182845 \cdots$, buscar los primos reducidos para el número e.

6. Resolver en números enteros las ecuaciones siguientes:

a) $5x + 4y = 3$; b) $7x - 19y = 5$; c) $12x - 7y = 15$.

§4. Sistema de Enteros

Sistema de enteros. Sean g un número natural superior a 1 y $M = \{0,1, \cdots, g-1\}$. Decimos que el número natural a se escribe en un sistema de posición de la base g si

$$(1)\ a = a_s g^s + a_{s-1} g^{s-1} + \cdots a_1 g + a_0,$$

donde$s$ es un entero no negativo, $a_0, \cdots, a_s \in, M$ y $a_s \neq 0$.

Si cada número del conjunto $M = \{0,1, \cdots, g-1\}$ se designa por símbolo especial, estos símbolos entonces se llaman *cifras del sistema g-nario de posición*. La representación (1) entonces se escribe bajo la forma simplificada

$a = (a_s a_{s-1} \cdots a_1)_g$

y se llama *notación del sistema g-nario de posición*. Es así como la notación

$a = (2315)_{10}$ significa que $a = 2.10^3 + 3.10^2 + 1.10 + 5$,

la notación

$b = (101001)_2$ significa que $b = 1.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 0.2^1 + 1$.

TEOREMA 4.1. *Sean g un número natural dado superior a la unidad y* $M = \{0,1,\cdots, g-1\}$. *Todo número natural* a *representada de manera única bajo la forma*

$(1) a = a_s g^s + a_{s-1} g^{s-1} + \cdots a_1 g + a_o$,

donde $a_i \in M$ y $a_s \neq 0$.

Demostración. La existencia de la representación (19 se demuestra por recurrencia en a. Si $a = 1$ o $a < g$ la igualdad $a = a$ es la representación buscada. Sea $a \geq g$; supóngase que para todos los números naturales inferiores a a se estableció la posibilidad de representación (1). Dado que $a \geq g$, que divide a por g con residuo, resulta

$(2) a = bg + a_0$, donde $a_0 \in M$ y $1 \leq b < a$.

Ya que $b < a$, según la hipótesis de recurrencia, el numero b representable bajo la forma

$(3) b = a_s g^{s-1} + \cdots + a_2 g + a_1$, donde $a_1, \cdots, a_s \in M$ y $a_s \neq 0$.

Refiriéndose a la expresión (3) de b en el segundo miembro de (2), resulta la representación para el número a,

$a = a_s g^s + \cdots + a_1 g + a_0$, donde $a_i \in M$ y $a_s \neq 0$,

Se denomina *descomposición del número a en potencias del número g*.

Demuéstrese la univocidad de la representación por recurrencia en a. Si $1 \leq a < g$, vemos sin duda que hay univocidad. Supóngase que la univocidad se demostrado para todos los números naturales inferiores a a. Admítase que además de (1) existe para a otra representación:

$(4) a = a'_{s'} g^{s'} + \cdots + a'_1 g + a'_0$.

Conforme a (1) y (4), se obtiene

$$(5) a = g(a_s g^{s-1} + \cdots + a_2 g + a_1) + a_0 = g\left(a'_{s'} g^{s-1'} + \cdots + a'_s g + a'_1\right) a'_0.$$

De (5), conforme a la univocidad de la división con residuo, se deduce que

$a_0 = a'_0$

$b = a_s g^{s-1} + \cdots + a_2 g + a_1 = a'_{s'} g^{s-1'} + \cdots + a'_2 g + a'_1.$

Como $b < a$, por hipótesis de recurrencia, $s = s'$ y $a_i = a'_i$ para $i = 1, \cdots, s$. □

Operaciones aritméticas en los enteros sistemáticos. Si los números naturales se escriben en el sistema de numeración decimal utilizamos entonces las reglas de adición y de sustracción en << columnas >>. Las operaciones de adicción y de sustracción de los enteros multivalentes en el sistema de numeración de g-nario se efectúan que sigue las mismas reglas que en la numeración decimal. En la numeración g-nario, como en la decimal, adicionándose los números multivalentes adicionamos primeramente las unidades, luego pasamos al orden que sigue, etc., hasta el orden que domina en presencia. Además, cada vez que la suma de un orden anterior es superior a la basa g del sistema de numeración o esta es igual, es necesario hacer un cambio al orden que sigue.

Los ejemplos siguientes ilustran las operaciones de adicción en los sistemas de numeración de base 6 y binario:

$$\begin{array}{r} (4253)_6 \\ +\,(2542)_6 \\ \hline (11235)_6 \end{array} \qquad \begin{array}{r} (10011)_2 \\ +\,(11001)_2 \\ \hline (101100)_2 \end{array}$$

La sustracción en la numeración quinaria ilustrada por ejemplo

$$\begin{array}{r} (42044)_5 \\ -\,(23141)_5 \\ \hline (13403)_5 \end{array}$$

La operación de multiplicación de los enteros multivalentes en numeración g-naire se efectúa siguiendo las mismas reglas que en la numeración decimal (<< en columnas>>). Al efectuar la multiplicación es práctico servirse de las tablas de multiplicación. Dadas más debajo de la tabla de multiplicación del sistema de numeración de base 6. Cada celda de esta tabla contiene el producto de números que representa los números de la línea y de la columna cuya intercesión es la misma celda, todos los números que figura en el sistema de numeración de base 6.

El ejemplo que sigue sirve de ilustración de la multiplicación (<< en columnas>>) en el sistema de numeración de base 6:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

$$\begin{array}{r} x_{343}^{235} \\ \hline 1153 \\ 1432 \\ 1153 \\ \hline 135213 \end{array}$$

Transferencia de números de un sistema de numeración al otro.

Supóngase que el número a se escribe en el sistema de numeración $m - naire$. Esta significa que se representa bajo la forma de una suma:

(1) $\mathrm{a} = \mathrm{b_k m^k} + \mathrm{b_{k-1} m^{k-1}} + \cdots \mathrm{b_1 m} + \mathrm{b_0}$.

¿Cómo transcribir este número en otro sistema cualquiera, dígase, en el sistema g-naire? Esto significa que es necesario representar el número a bajo la forma

(2) $a = a_s g^s + a_{s-1} g^{s-1} + \cdots + a_1 g + a_0$.

Para esto se debe encontrar los coeficientes $a_0, a_1, \cdots, a_s$ cuyo cada uno es un cifra que va de 0 a g-1 incluido. Divídase el número a dado en numeración $m - naire$ por g, obténgase el residuo a_0 y el cociente q_1. Luego divídase el cociente q_1 por g y obténgase el residuo a_1 y el cociente q_2. La operación se continúa hasta que solo obtengamos un residuo igual a cero. Finalmente, se obtiene todas las cifras $a_0, a_1, \cdots, a_s$ que entra en la representación de g-naire (2) del número a.

A modo de ejemplo estúdiese la transferencia del número $a = (5\ 3\ 7\ 8)_{10}$ en el sistema de numeración de base 6. Al dividir por 6, se obtiene el cociente 896 y el residuo 2. Así pues en la numeración de base 6 la última cifra del número a es 2. Para encontrar la segunda cifra divídase el cociente 896 por 6. Se obtiene el cociente 149 y residuo 2. La segunda cifra en numeración base 6 del número a es 2. Luego, divídase 149 por 6, se obtiene el cociente 24 y el residuo 5. Este residuo es la tercera cifra del número a en la numeración base 6. Finalmente, divídase el cociente 24 por 6, se obtiene el cociente 4 y 0 como residuo. Así pues,

$(5\ 3\ 7\ 8)_{10} = (4\ 0\ 5\ 2\ 2)_6$.

Ejercicios

1. Formar la tabla de multiplicación del sistema de numeración septenaria.
2. Demostrar que $A = (a_n a_{n-1} \cdots a_1 a_0)_{12}$ es divisible para 8 (por 9) si es divisible por 8 (9) el número $(a_1 a_0)_{12}$ formado con sus dos últimas cifras.
3. Mostrar que el número $A = (a_n a_{n-1} \cdots a_1 a_0)_g$, es decir el número $a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$ es divisible por g-1 si g-1 es divisible para la suma de sus cifras, es decir la suma $a_n + a_{n-1} + \cdots + a_1 + a_0$.
4. Demostrar que un número natural cuya numeración decimal se compone de 3^n unidades es divisible por 3^n.
5. En la numeración decimal de un número natural hay 30 unidades, las cifras restantes que son de ceros. Este número puede ser un cuadrado perfecto?
6. Le gustaría conocer mi número de teléfono para aquellas preguntas que solo responderé con un <<si>> y<< no>>. Encontrar el proceso que garantice el éxito para el menor número posible de preguntas (el número del teléfono se compone de cinco cifras arbitrarias).

§ 5. Distribución de números primos

Distribución de números primos. Designase por $\pi(x)$el número de primos positivos inferiores al número real x. Se establecido al §1 que existe una infinidad de números primos (TEOREMA de Euclides).
Como resultado, $\pi(x) \to \infty$ para $x \to \infty$.

En 1808 Le Gendre publicó la fórmula empírica que había encontrado para la representación aproximada de la función $\pi(x)$. Le Gendre formuló la proposición que para los grandes valores de $x\pi(x)$ vale aproximadamente $\frac{x}{\log x - 1{,}08366}$.

Tchébychev mostró en 1849 la falla de esta afirmación. En los trabajos publicados en 1848 y 1850 Tchébychev estableció la relación de la función $\pi(x)$ con la relación $\frac{x}{logx}$. Demostró el TEOREMA siguiente: *existe constantes positivas* a *y* b, $a < b$, *tales como para cualquier* x *suficientemente grandes se obtuvo*

(1) $a.\frac{x}{\log x} < \pi(x) < b\,\frac{x}{log\ x}$.

Realizamos más adelante la demostración del TEOREMA: para cualquier $x \geq 2$ tenemos las desigualdades

(2) $log2.\frac{x}{logx} - 2 < \pi(x) < 4\log 2\ \frac{x}{logx} + log_2 x$.

En la base de las desigualdades (2) se está en condición de obtener las constantes a y b de las desigualdades (1).

Para demostrar las desigualdades (2) se introdujo la función $T(x) = log[x]!$ y se estableció las que aumenten y las que disminuyen de la función $T(x) - 2T\left(\frac{x}{2}\right)$.

Funciones $\boldsymbol{T(x)}$ y $\boldsymbol{\Lambda(x)}$. El símbolo $\Lambda(x)$ designa la función cuyo valor es $\log p$, si n es un número primo o un exponente positivo del número primo p, en los otros casos su valor es cero

$$\Lambda(n) = \begin{cases} \log P \ si\ n = P^m\ para\ todo\ número\ natural\ m > 0, \\ 0\ si\ n \neq P^m. \end{cases}$$

A continuación se utilizara la propiedad siguiente de esta función:

$$(1)\sum_{d/n} \Lambda(\mathrm{d}) = \log \mathrm{n}.$$

$Sea\ n = \prod_{p/n} p^{e\ p}$ la descomposición canónica del número natural n. Se ve fácilmente que

$$\sum_{d/n} \Lambda(d) = \sum_{p^{x/n}} \log P = \sum_{p/n} e_p \log P = \log n,$$

donde P^α recorre todas las potencias de números primos incluidos en n.

El símbolo $T(x)$ designa la función que para todo número real $x \geq 0$ toma el valor log $[x]!$, es decir

$$T(x) = log[x]! = \textstyle\sum_{n \leq x} \log n,$$

donde$[x]$ es la parte entera del número x.

Al sumar (1) en todo los enteros positivos $n \leq x$, se obtuvo

$$\sum_{m \leq x} \Lambda\,(m)\left[\frac{x}{m}\right] = \sum_{n \leq x} \log n = \log[x]\,! = T(x).$$

Así se demostró la proposición siguiente.

PROPOSICIÓN 5.1. Para todo número real $x \geq 1$

$$(1) T(x) = \sum_{m \leq x} \Lambda(m) \left[\frac{x}{m}\right]$$

Desigualdades impuestas a la función $T(x)$. Por definición de la función $T(x)$,

(1) $T(n) = \log n!$,

para todo x real positivo

(2) $T(x) = log[x]!$

Debido a (1), se tiene

(3) $T(2n) - 2T(n) = log \frac{(2n)!}{(n!)^2} = log C_{2n}^n$.

Demuéstrese que para todo número natural $n \geq 2$ se cumplen las desigualdades

$$(4) \frac{4^n}{2n} < C_{2n}^n < 4^n.$$

Se ve sin duda que $C_{2n}^n < (1+1)^{2n} = 4^n$. Los cálculos que siguen demuestran la segunda desigualdad de:

$$C_{2n}^n = \frac{2n(2n-1)(2n-2)\cdots 2.1}{n^2(n-1)^2\cdots 1^2} =$$
$$= \frac{2n(2n-1)}{n^2} \cdot \frac{(2n-2)(2n-3)}{(n-1)^2} \cdots \frac{2.1}{1^2} =$$
$$= 4^n \left(1 - \frac{1}{2n}\right)\left(1 - \frac{1}{2(n-1)}\right) \cdots \left(1 - \frac{1}{2}\right) =$$
$$= 4^n \cdot \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} > 4^n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} = \frac{4^n}{2n}.$$

A partir de (3) conforme a (4), resulta para $n \geq 2$ las desigualdades

$$(5) T(2n) - 2T(n) < log 4^n = 2n\, log 2,$$

$$(6) T(2n) - 2T(n) > log \frac{4^n}{2n} = 2n\, log 2 - log 2n.$$

Sea x un número real cualquiera superior o igual a 2 y sea $2n$ el máximo número par que no supere$x$. Entonces, de la igualdad (2) deriva

$$(7) T(x) - T(2n) \leq \log x.$$

$T(x)$que es una función no creciente, resulta de (5) y (7)

(8) $T(x) - 2T\left(\frac{x}{2}\right) < x\ lox2 + logx.$

Conforme a (6),

$$T(x) - 2T\left(\frac{x}{2}\right) > (x-2)\ lox2 - log\mathrm{x}$$

De ahí, para $x \geq 4$, se obtiene la desigualdad

(9) $T(x) - 2T\left(\frac{x}{2}\right) > x\ log2 - 2\log x \qquad (x \geq 4).$

Desigualdades de Tchébychev. Se obtuvo anteriormente (ver la desigualdad (8)) la desigualdad

(1)$T(x) - 2T\left(\frac{x}{2}\right) < x\ log2 + \log x$

Y se demostró la desigualdad

$(2)T(x) = \sum_{m \leq x} \Lambda(m)\left[\frac{x}{m}\right].$

Si $\frac{x}{2} < m \leq x$, entonces $2m > x$. también de la desigualdad $\left[\frac{x}{m}\right] = 1$resulta $\left[\frac{x}{2m}\right] = 0$. De ahí y a partir de (2), se obtuvo:

$(3)T(x) - 2T\left(\frac{x}{2}\right) = \sum_{m \leq x} \Lambda(m)\left(\left[\frac{x}{m}\right] - 2\left[\frac{x}{2m}\right]\right) \geq$

$$\geq \sum_{\frac{x}{2} < m \leq x} \Lambda(m) \geq \sum_{\frac{x}{2} < p \leq x} \log p \geq \log\left(\frac{x}{2}\right)\left[\pi(x) - \pi\left(\frac{x}{2}\right)\right].$$

Conforme a (2) y (3), se obtuvo

(4) $\left(\pi(x) - \pi\left(\frac{x}{2}\right)\right)\ log\frac{x}{2} < x\ log2 + \log x.$

Se deduce de esta desigualdad que sustituye sucesivamente a x

$\frac{x}{2}, \frac{x}{4}, \frac{x}{8}, \cdots$ una serie de desigualdades:

$(4')\left(\pi\left(\frac{x}{2}\right) - \pi\left(\frac{x}{4}\right)\right) log\frac{x}{4} < \frac{x}{2} log2 + log\frac{x}{2},$

$(4'')\left(\pi\left(\frac{x}{4}\right) - \pi\left(\frac{x}{8}\right)\right) log\frac{x}{8} < \frac{x}{4} log2 + log\frac{x}{4}.$

. . . . . .

Al sumar los primeros miembros de las desigualdades (4),$(4')$, $(4'')$, $\cdots$, se obtuvo

$$\pi(x)log\frac{x}{2}\pi\left(\frac{x}{2}\right)\left(log\frac{x}{2}-log\frac{x}{4}\right)-$$

$$-\pi\left(\frac{x}{4}\right)\left(log\frac{x}{4}-log\frac{x}{8}\right)-\cdots=$$

$$=\pi(x)logx-\left(\pi(x)+\pi\left(\frac{x}{2}\right)+\pi\left(\frac{x}{4}\right)+\cdots\right)log2>$$

$$>\pi(x)logx-\left(x+\tfrac{x}{2}+\tfrac{x}{4}+\cdots\right)log2=$$

$$=\pi(\pi)logx-2xlog2.$$

La suma de los segundos miembros de las desigualdades (4),$(4')$, $(4'')$, $\cdots$ será inferior a $2xlog2+logx.log_2x$, dado que el número de desigualdades no supera log_2x. Se logra así la desigualdad

$$\pi(x)logx-2xlog2<2xlog+logx.log_2x,$$

de donde

$$\pi(x)<4\,log2\frac{x}{logx}+log_2x.$$

Además, la desigualdad obtenida se efectúa para todo $x\geq 2$.

Se demostró anteriormente la desigualdad

$$T(x)=2T\left(\frac{x}{2}\right)>x\,log2-2\log x.$$

Además, dado que $T(x)-2T\left(\frac{x}{2}\right)=\sum_{m\leq x}\Lambda(m)\left(\left[\frac{x}{m}\right]-\left[\frac{x}{2m}\right]\right)$, se tiene

$$T(x)-2T\left(\frac{x}{2}\right)\leq\sum_{m\leq x}\Lambda(m)=\sum_{p\leq x}\left[\frac{logx}{logp}\right]\log\,p\leq$$

$$\leq\sum_{p\leq x}\frac{logx}{logp}logp\leq\pi(x)logx$$

Así, $x\,log2-2logx<\pi(x)logx$. Por consiguiente, para todo $x\geq 2$

$$log2\frac{x}{logx}-2<\pi(x),$$

Es decir que se obtuvo el límite inferior de la forma buscada para $\pi(x)$.

Así se demostró el TEOREMA que sigue.

TEOREMA 5.2. Para cualquier $x\geq 2$ se tiene:

$$log2\frac{x}{logx}-2<\pi(x)<4\,log2\frac{x}{logx}+log_2(x).$$

En 1850, Tchébychev demostró las desigualdades más estrictas. También demostró que para las x suficientemente grandes se satisface las desigualdades

$$(0,92\ldots)\frac{x}{\log x} < \pi(x) \leq (1,105\ldots)\frac{x}{\log x}.$$

Al demostrar estas desigualdades Tchébychev en lugar de $T(x) - 2T\left(\frac{x}{2}\right)$ se sirvió de una expresión más compleja:

$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{30}\right).$$

En 1851, Tchébychev emitió la hipótesis sobre la dependencia entre $\pi(x)\ y\ \frac{x}{\log x}$;

$$lim\frac{\pi(x)}{x/\log x} \leq 1 \leq lim\frac{\pi(x)}{x/logx}$$

de modo que si el límite de la relación $\frac{\pi(x)}{x/\log x}$ existe, es igual a 1.

El resultado fundamental de la teoría de números es la ley asintótica de la distribución de números primos demostrados por primera vez en 1896 por Hadamard y la Vallée-Poussin.

Esta ley estipula que *la relación* $\pi(x)$*:* $\frac{(x)}{x/\,log\,x}$ *tiende hacia 1 cuando* x *de forma indefinida,* es decir,

$$\lim_{x \to \infty} \frac{\pi(x)\log x}{x} = 1.$$

Números primos de las progresiones aritméticas. Estúdiese tres teoremas (5.3-5.5) que constituyen de casos particulares de un TEOREMA más general- el TEOREMA de Dirichlet.

TEOREMA 5.3. *La secuencia aritmética* $4n + 3(n = 0,1,\ldots)$ *contiene una infinidad de números primos.*

Demostración. Considérese el número M definido por la igualdad $M = 4n! - 1$ donde n es un entero positivo. M Es un número de la forma $4k + 3$, puede componerse solamente de factores primos de la forma $4k + 1$, ya que el producto de números de la forma $4k + 1$ es un número de forma idéntica:

$$(4k + 1)(4k_1) = 4(4kk_1 + k + k_1)\ + 1.$$

Luego, el número M posee al menos un factor primo de la forma $4k + 3$ superior a n. Así, para cada número natural n existe un número primo superior a n y que tiene la forma $4k + 3a \equiv b(modulo\ m)$

TEOREMA 5.4. *La secuencia aritmética* $6n + 5(n = 0,1,2,\ldots)$ *contiene una infinidad de números primos.*

Demostración. Este TEOREMA se demuestra de manera análoga en el anterior. Considérese el número M definido por la igualdad $M = 6n! - 1$, donde n es un entero positivo cualquier; M es un número de la forma $6k + 5$. El número $\boldsymbol{M}$ puede ser únicamente compuesto de factores primos de la forma $6k + 1$, ya que el producto de números de la forma $6k + 1$ es un número de forma idéntica:

$$(6k + 1)(6k_1 + 1) = 6(6kk_1 + k + k_1) + 1.$$

Como resultado, el número M posee al menos un factor primo superior a n ya que tiene la forma $6k + 5$. ■

TEOREMA 5.5. La secuencia aritmética

$4n + 1 \quad (n = 0,1,2, \dots)$

contiene una infinidad de números primos.

Demostración. Sea n todo número natural superior a la unidad. Entonces, $(n!)^2 + 1$, siendo número impar, es mayor que la unidad que posee un factor primo impar p*; p,* ya que de la forma $4k + 1$ o $4k + 3$. Plantéese que $p = 4k + 3$. Dado que para las a naturales y los m impares

$a + 1 | a^m + 1)$, se tiene $(n!)^2 + 1 \quad |n!)^{2(2R+1)} + 1$.

Como $2(2k + 1) = 4k + 2 = p - 1$ y

$p|(n!)^2 + 1$, se tiene $p|(n!)^{p-1} + 1$.

Por consiguiente,

(1) $p|(n!)^p n!$

Por otro lado, según el TEOREMA de Fermat

(2) $p|(n!)^p - n!$

Se deduce de (1) y (2) que $p|2(n!)$, lo que es imposible, ya que p es un número primo impar superior a n. Por consiguiente, p debe ser un número natural de la forma $4k + 1$. Se demuestra que para todo número natural n existe un número primo superior a n y que tenga la forma $4k + 1$. □

Los TEOREMAs demostrados anteriormente son los casos particulares del TEOREMA de Dirichlet en las progresiones aritméticas: *toda secuencia aritmética* $a + km(k = 0,1,2, \dots)$ *donde* $(a, m) = 1$ *contiene una infinidad de números primos*.

Ejercicios

1. Mostrar que el polinomio $x^2 + x + 41$ luego de la secuencia de números $x = 0,1,2, \dots ,39$ de valores que son de números primos distintos.
2. Sea f un polinomio en x de la potencia positiva de coeficientes enteros. Demostrar que para el número infinito de x naturales el número $f(x)$ es un número compuesto.
3. Al apoyarse del TEOREMA de Dirichlet sobre las progresiones aritméticas, demostrar que para todo número natural m existe un número primo en la que la imagen gráfica (en el sistema de numeración decimal u otro sistema de numeración de base natural $q > 1$) contiene menos m ceros.

CAPITULO XII
TEORIA DE CONGRUENCIAS CON FUNCIONES ARITMÉTICAS

§1. Congruencias y sus propiedades.

Congruencias en un anillo de enteros. Sea $\mathcal{Z}$ un anillo de entero, m un entero fijo y $m\boldsymbol{Z}$ el conjunto de todos los enteros múltiples de m.

DEFINICIÓN. Dos enteros $a\ y\ b$ se denominan *módulo congruente* m si m divide $a - b$

Si $a\ y\ b$ son módulo congruente m, se denota de la siguiente manera:

(1) $a \equiv b(módulo\ m)$

La congruencia de módulo m posee las propiedades de reflexividad, de simetría y transitividad, es decir, es una relación de equivalencia. Por lo tanto, la congruencia induce la parte del conjunto $\boldsymbol{Z}$ de los enteros en clases de equivalencias que se denomina *clases residuales de módulo m.*

Nótese que la congruencia de módulo m coincide con la congruencia de módulo $(-m)$. La congruencia de módulo 0 coincide con la relación de igualdad. Dos enteros cualesquiera son congruencias de módulo 1.

Como la congruencia de módulo m es una relación de equivalencia en el conjunto $\boldsymbol{Z}$**,** las clases de equivalencia, es decir, las clases residuales de módulo m, poseen las propiedades siguientes:

PROPIEDAD 1.1. Ambas clases residuales de módulo m o bien coinciden, o bien son disjuntas. La reunión de todas clases residuales de módulo m coincide con el conjunto $\boldsymbol{Z}$ de todos los enteros.

PROPIEDAD 1.2. Sea A y B clases residuales de módulo m $a \in A\ y\ b\ \in B$. Las clases A y B según un sub-grupo coinciden si y sólo si $a \equiv b(módulo\ m)$.

PROPIEDAD 1.3. Si A es una clase residual de módulo m y a un elemento cualquiera de A, entonces $A = a + m\boldsymbol{Z}$, es decir, $A = \{a + mk | k \in \boldsymbol{Z}\}$.

PROPOSICIÓN 1.1. Los números $a\ y\ b$ son congruentes de módulo $m(m \neq 0)$ si y sólo si después de dividir por m dan lugar a los residuos idénticos.

Demostración. Supóngase que después de la división con residuo de los números $a\ y\ b$ por m se obtienen los cocientes $q\ y\ q_1$ y los residuos $r\ y\ r_1$,

$$a = qm + r, 0 \leq r < m; b = q_1 m + r_1, 0\ \leq r_1 < m$$

Plantéese que $r > r_1$. la segunda igualdad se extrae de la primera, y se tiene

(1) $a - b = (q - q_1)m + (r - r_1),\ \ 0 \leq r - r_1 < m.$

Si $a \equiv b(módulo\ m)$, entonces, por definición de la congruencia, $a - b$ es divisible por m, luego $r - r_1 = 0\ y\ r - r_1$. Por otra parte si $r = r_1$, entonces, en virtud de (1), $a - b$ es divisible por m
Es decir, $a \equiv b(módulo\ m)$□

Propiedades básicas de congruencias. Varias propiedades de las congruencias son análogas a las propiedades de las igualdades.

PROPIEDAD 1.4. *Las congruencias pueden adicionarse y sustraídas parte por parte, es decir, si* $a \equiv b(módulo\ m)$*,* $c \equiv d(módulo\ m)$*, entonces,* $a + c \equiv b + d\ (módulo\ m)$*.*

Demostración. Por hipótesis, $m|(a - b)$ y $m|(c - d)$. Por tanto $m|(a - b) \pm (c - d), m|(a + c) - (b + d)$ y $m|(a - c) - (b - d)$.□

PROPIEDAD 1.5. *Las congruencias pueden multiplicarse parte por parte, es decir, si* $a \equiv b(módulo\ m)$*,* $c \equiv d(módulo\ m)$*, entonces,* $ac \equiv bd(módulo\ m)$.

En particular, las dos partes de la congruencia pueden multiplicarse por el mismo entero.

Demostración. Por hipótesis, $a - b \in m\boldsymbol{Z}$ y $c - d \in m\boldsymbol{Z}$. Por lo tanto, $ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d \in)m\boldsymbol{Z}$**,** es decir, $ac \equiv bd(modulo\ m)$. □

PROPIEDAD 1.6. *Las dos partes de la congruencia pueden dividirse por el factor común si este último y el módulo son primos entre ellos.*

Demostración. Si $ca \equiv cb(módulo\ m)$, es decir, $m|c(a-b)$ y los números c y m son primos entre ellos, entonces m divide $a-b$. Por consiguiente, $a \equiv b\ (módulo\ m)$. □

PROPIEDAD 1.7. *Las dos partes de la congruencia y el módulo pueden ser divididos por su común divisor.*

Demostración. Si $ka \equiv kb(modulo\ mk)$, entonces $k(a-b)$ se divide por km. Por consiguiente, $a-b$ es divisible por m, es decir, $a \equiv b\ (modulo\ m)$. □

PROPIEDAD 1.8. *Sea m_1 un divisor cualquiera de m. Si $a \equiv b(módulo\ m)$, entonces, $a \equiv b\ (módulo\ m_1)$.*

Demostración. Si $a \equiv b(módulo\ m)$, entonces, $a-b$ es divisible por m. Ahora bien, m_1 es un divisor de m, por tanto, $a-b$ se divide por m, es decir, $a \equiv b\ (módulo\ m_1)$. □

Ejercicios

1. Mostrar que todo número natural transcrito en numeración decimal es congruencia de módulo 9 y de módulo 3 con la suma de sus cifras.
2. Establecer la regla de verificación por 9 de operaciones aritméticas.
3. Buscar los caracteres de divisibilidad por 9 y 19 de números del sistema de numeración
4. decimal.
5. Buscar los caracteres de divisibilidad para 2, 3, 4, 5, 7,9 en el sistema de numeración octal.
6. Buscar los caracteres de divisibilidad para 2, 3, 4, 5, 6, 7, 8, 11,13 en el sistema de numeración dodecimal.
7. Demostrar que sí $a \equiv b(módulo\ m)$, $a \equiv b(módulo\ n)$, y m, n de números primos entre ellos, se tiene $a \equiv b(módulo\ mn)$.
8. Sea d el máximo común divisor de enteros m y n. Demostrar que si $a \equiv b(módulo\ m)$ y $a \equiv b(módulo\ n)$, entonces $a \equiv b(módulo\ \frac{mn}{d})$.

§ 2. Sistema completo de residuos.

Sistema completo de residuos. Según la propiedad 1.1 cada clase residual de módulo m se define de manera univoca para todo número a que pertenece a esta clase; esta clase es un conjunto de todos los números de la forma $a+km$, es decir, es el conjunto

$$\{a+km|k \in \mathrm{Z}\} = a + m\mathrm{Z}.$$

La clase residual de módulo m que comprende el número a, es decir, la colección de todos los enteros b por ejemplo $b \equiv a(módulo\ m)$ se denota simplemente $a\ módulo\ m$:

$$a\ módulo\ m = \{a+km|k \in \mathrm{Z}\}.$$

Todo número que pertenece a la clase residual $a\ módulo\ m$ se denomina *representante de esta clase.*

DEFINICIÓN. Se denomina *sistema completo de residuos de módulo* m la colección de m enteros que representa estrictamente un representante de cada clase residual módulo m.

Cada clase residual de módulo m contiene estrictamente uno de los números de la colección de todos los residuos posibles de la división para m, al saber que, 0, 1,2,…, $m-1$.

DEFINICIÓN. La colección de números 0, 1,2,…, $\mathrm{m}-1$ se denomina *sistema de residuos mínimos no negativo módulo0, 1,2,…, m.*

Por otro lado más adelante la notación $(a\,,m)=1$ significará que los números $a\ y\ m$ son primos entre ellos.

PROPOSICIÓN.2.1. *Toda colección de m número $(a\ >1)$ no congruente ambos módulo m que constituyen un sistema completo de residuos de módulo m.*

Demostración. Sea M la colección de m números no congruente de ambos módulo m. Entonces, los números que pertenecen a clases residuales diferentes. A demás, M comprende m números. Por consiguiente, el conjunto M contiene un representante de cada clase residual módulo m. □

PROPOSICION 2.2. *Sea $a\ y\ b$ enteros y $(a\,,m)=1$. Si x recorre el sistema completo de residuos módulo m, entonces, $ax+b$ recorre también el sistema completo de residuos de módulo m.*

Demostración. Sea M el sistema completo de residuos. Entonces, el conjunto $M_1=\{ax+b|x\in M\}$ contiene, como M, m elementos. Ambos números ax_1+b y ax_2+b de M son no congruente si $x_1\not\equiv(módulo\ m)$. Así que, el conjunto M_1 es un sistema completo de residuos de módulo m.□

Grupo aditivo de clases de residuos. Desígnese por $\mathrm{Z}\ /\ m\mathrm{Z}$ el conjunto de todas las clases residuales módulo m:

$$\mathrm{Z}\ /\ m\mathrm{Z}=\{0\ módulo\ m, 1\ módulo, \dots, (m-1)módulo\ m\}.$$

Defínase las operaciones $+,-$ en el conjunto de clases residuales de la manera siguiente:
$a\ módulo\ m+b\ módulo\ m=(a+b)módulo\ m, -(a\ módulo\ m)=(-a)módulo\ m.$
Según las propiedades 1.4 y 1.5 de congruencias, la congruencia aplicada en el conjunto Z es una congruencia con respecto en la operación de adición en Z y la operación de paso al elemento opuesto. Así, ambas clases cualesquiera a módulo m y b módulo m independientemente de la elección de representantes $a\ y\ b$ en su seno se asocia de manera univoca la clase $(a+b)módulo\ m$ que es su suma. De manera análoga, la clase $-(a\ módulo\ m)$ es independiente de la elección del representante a.Dado que la adición de enteros es conmutativa y asociativa, la adición de clases de residuos es también conmutativa y asociativa, es decir, para todos $a,b,c\ \in Z$

$$a\ módulo\ \ m+b\ módulo\ m=b\ módulo\ m+a\ módulo\ m, (a\ módulo\ m+b\ módulo\ m)+c\ módulo\ m=a\ módulo\ m+\ (b\ módulo\ m+c\ módulo\ m).$$

La clase de residuos $0\ módulo\ m$ es un elemento neutro conforme a la adición, es decir para cualquier clase de residuos $a\ módulo\ \ m$

$$a\ módulo\ \ m+0\ módulo\ m=a\ módulo\ m.$$

Luego, las clases $a\ módulo\ m$ y $(-a)módulo\ m$ son mutuamente opuestas, es decir,

$$a\ módulo\ m+(-a)módulo\ m=0\ módulo\ m.$$

Se establece por tanto el TEOREMA siguiente.

TEOREMA 2.3. *El algebra $\langle \boldsymbol{Z}|m\boldsymbol{Z},+,-\rangle$ constituye un grupo. Este grupo es un grupo cociente del grupo $\mathcal{Z}$ seguido el sub-grupo $m\mathcal{Z}$.*

DEFINICIÓN. El grupo $\langle \boldsymbol{Z}|m\boldsymbol{Z},+,-\rangle$ *se denomina grupo aditivo de clases residuales módulo m.*

Anillo de clases residuales. Sobre el conjunto de clases residuales módulo m defínase la multiplicación de la manera siguiente:

$$(a\ módulo\ m)\ \cdot (b\ módulo\ m) = ab\ módulo\ m.$$

Según la propiedad 1.5 de congruencias, la congruencia módulo m sobre $\boldsymbol{Z}$ es una congruencia con respecto en la operación de multiplicación sobre $\boldsymbol{Z}$**.** Por lo tanto, en cada dos clase residuales $a\ módulo\ m\ y\ b\ módulo\ m$, independientemente e la elección en su seno de representantes a, b se asocian de manera univoca. La clase residual $ab\ módulo\ m$ que es su producto. Dado que las operaciones de adición y de multiplicación de clases residuales se reducen a las operaciones apropiadas sobre los números de estas clases residuales, estas operaciones respetan las leyes de adición y de la multiplicación, en particular, las leyes de conmutativa, asociativa y distributiva

$(a\ módulo\ m)(b\ módulo\ m) = (b\ módulo\ m)(a\ módulo\ m),$
$(a\ módulo\ m)[(b\ módulo\ m)(c\ módulo\ m)] = [(a\ módulo\ m)(b\ módulo\ m)](c\ módulo\ m)$
$(a\ módulo\ m)(b\ módulo\ m) + (c\ módulo\ m)] = (a\ módulo\ m)(b\ módulo\ m) + (a\ módulo\ m)(c\ módulo\ m).$

A demás, la clase residual 1 módulo m es un elemento neutro con respecto a la multiplicación:
$(a\ módulo\ m)(1\ módulo\ m) = a\ módulo\ m.$

El TEOREMA siguiente posteriormente se verifica.

TEOREMA2.4 El algebra $\langle \boldsymbol{Z}|m\boldsymbol{Z}, +, -, \cdot, \boldsymbol{1\ módulo\ m}\rangle$ *es un anillo conmutativo (abeliano).*

DEFINICIÓN. El anillo $\langle \boldsymbol{Z}|m\boldsymbol{Z}, +, -, \cdot, \boldsymbol{1\ módulo\ m}\rangle$ se denomina *anillo de clases residuales de módulo* m*.*

Ejercicios.

1. Buscar el sistema completo de residuos y el sistema absolutamente el menor residuo de módulo 30.
2. Buscar el sistema completo absolutamente menor del residuo de módulo 19.
3. Las potencias 2^0, 2^1, 2^2,…, 2^{10} con el numero 0 forman un sistema completo de residuos de módulo 11?
4. Al llevar en la expresión $3x + 7y$ los valores $x = 0,1,2,3,4,5,6$ y de $y = 0,1,2$ verificar que tendremos finalmente un sistema completo de residuos módulo 21.

§3. Sistema residual reducido

Sistema residual reducido: Sea n un número positivo cualquiera. Nótese $\varphi(n)$ el número enteros positivos no supera n y primos con n. El máximo común divisor de enteros a, b que es un número natural se denotará a, b.

PROPOSICIÓN 3.1. *Todos los números de la clase residual fijo* $a\ módulo\ m$ *posee con* m *un mismo máximo común divisor, igual a* (a, m).

Demostración. Si b es un número natural cualquiera de la clase residual $a\ módulo\ m$, entonces, $b = mq + a$ donde q es cualquier entero. Por lo tanto, en virtud de la proposición 11.3.1, se deduce que $(b, m) = (a, m)$. □

Por consiguiente, (a, m) depende únicamente de la clase residual $a\ módulo\ m$ y es independiente de la elección del representante a en esta clase. En particular, si $(a, m) = 1$, la clase $a\ módulo\ m$ se denomina *clase residual que constituye un elemento primo con el módulo* m*.*

PROPOSICIÓN 3.2. *El número de clases residuales, que forma con* m *los elementos primos, vale* $\varphi(m)$*.*

Demostración. A partir del sistema completo de residuos módulo m

$1, 2, \dots, m$

Se deriva el sistema de todos los residuos primos con m:

$a_1, a_2, \dots, a_{\varphi(m)}$.

En virtud de la proposición 3.1, las clases residuales

$$(1)\ a_1\ módulo\ m,\ a_2\ módulo\ m, \dots,\ a_{\varphi(m)}\ módulo\ m$$

son elementos primos con el módulo m. Cualquier otra clase que no es en (1) no es primero con el módulo m, ya que contiene un elemento del conjunto $\{1, 2, \dots, m\} \setminus \{a_1, a_2, \dots, a_\varphi(m)\}$. Las clases que figuran en el sistema (1) son distintas. Por consiguiente, el número de clases que forman con m los elementos primos es $\varphi(m)$. □

DEFINICIÓN. Se denomina *sistema residual reducido módulo* m la colección de enteros que contienen un representante de cada clase residual, primo con m.

PROPOSICION 3.3. *Toda colección* $\varphi(m)$ *de números,* $m > 1$*, primos con* m *y ambos no congruente módulo* m *es un sistema residual reducido módulo* m*.*

Demostración. Sea M una colección $\varphi(m)$ de números primos con m y no congruente ambos módulo m. Estos números pertenecen entonces a clases residuales diferentes, por lo tanto el conjunto M encierra un representante de cada clase residual, primo con el módulo m. Por consiguiente, M es un sistema residual reducido módulo m. □

PROPOSICIÓN 3.4. *Sea* a *un entero positivo primo con* m *y* $b_1, b_2, \dots, b_{\varphi(m)}$ *un sistema residual reducido de módulo* m*, entonces, la colección* $ab_1, ab_2, \dots, ab_{\varphi(m)}$ *es también un sistema residual reducido de módulo* m*.*

Demostración. En razón de la proposición 3.3 se necesita demostrar que los números de la colección $ab_1, ab_2, \dots, ab_{\varphi(m)}$ ambos no son congruentes de módulo m. En efecto si $ab_i \equiv ab_\Re \times (módulo\ m)$ con $i \neq k$, se tiene entonces, según la condición $(a, m) = 1, b_i \equiv b_\Re (módulo\ m)$, lo que es imposible dado por la hipótesis de la proposición $b_i\ y\ b_\Re$ son elementos distintos del sistema residual reducido de módulo m. □

Grupo multiplicativo de clases residuales, elementos primos con el módulo. Considérese el TEOREMA con una propiedad muy importante de clases residuales, elementos primos con el módulo.

TEOREMA 3.5. *El conjunto de clases residuales de módulo* m *que forman elementos primos con módulo que constituyen con respecto a la multiplicación, un grupo abeliano.*

Demostración. Sea G_m el conjunto de todas las clases residuales de módulo m primos con m. El producto de dos clases residuales cualesquiera módulo m elementos primos con el módulo constituye una clase residual que forman elementos primos con el módulo y, luego el conjunto G_m es cerrado con respecto a la multiplicación. Luego, la operación de multiplicación de clases residuales es conmutativa y asociativa. La clase $\overline{1}, \overline{1} = 1\ módulo\ m$ es el elemento neutro con respecto a la multiplicación. Demuéstrese que pata cualquier clase $a \in G_m$ existe en G_m una clase inversa.

Sea $G_m = \{a_1, \dots, a_{\varphi(m)}\}$,

es decir que, $a_1, \dots, a_{\varphi(m)}$ es un sistema residual reducido de módulo m. Entonces, según la proposición 3.4 $aa_1, aa_2, \dots, aa_{(m)}$ es también un sistema residual reducido de módulo m; contiene entonces un número congruente con 1. Sea $ab_\Re \equiv 1(módulo\ m)$. Entonces $aa_\Re = 1$, y, que parte, $a_\Re$ es una clase inversa de la clase $a\ de\ G_m$. Así pues, el sistema $\langle G_m, ., -1\rangle$ es un grupo abeliano . □

DEFINICIÓN. El grupo $\mathcal{G}_m = \langle G_m, ., -1\rangle$ se denomina grupo multiplicativo de clases residuales módulo m, que forma con el módulo de elementos primos.

COROLARIO 3.6. *Si* p *es un número primo, entonces, el conjunto de clases residuales no nulos es un grupo abeliano con respecto a la multiplicación*.

TEOREMA 3.7. *Un anillo de clase residual módulo* m *constituye un cuerpo si y sólo si* m *es un numero primo.*

Demostración. Sea m un número primo, entonces, según el corolario 3.6, el conjunto de todas las clases residuales no nulos de módulo m es un grupo con respecto a la multiplicación.

También el anillo de las clases residuales de módulo m es un cuerpo.

Sea m es un número compuesto, $m = ab, 1 < a, b < m$. En este caso $(a\ módulo\ m)(b\ módulo\ m) = 0\ módulo\ m$, además, por la hipótesis,

$$a\ módulo\ m \neq 0\ módulo\ m, \qquad b\ módulo\ m\ \neq 0\ módulo\ m.$$

Así, el anillo de las clases residuales consta de divisores de cero y por consiguiente, no puede ser un cuerpo.

Si $m = 1$ el anillo de clases residuales módulo m es entonces un anillo reducido en $\{0\}$. Si por el contrario $m = 0$, el anillo de clases residuales módulo $m, \mathcal{Z} / (0)$, es isomorfa en el anillo $\mathcal{Z}$ y por consiguiente no es un cuerpo. □

DEFINICIÓN. El número a se denomina *inverso del número b módulo m* si $ab \equiv 1(modulo\ m)$. Los números $a\ y\ b$ serán igualmente denominados *mutuamente inverso de módulo m.*

PROPOSICION 3.8. *Sea a un número primo con el módulo m y $Pn - 1$ el numerador antepenúltimo reducido del número $\frac{m}{a}\left(\frac{m}{a} = \frac{P_n}{Q_n}\right)$. Entonces, $a(-1)n - 1\ Pn - 1 \equiv 1(módulo\ m)$, es decir, que el número $(-1)n - 1\ Pn - 1$ es la inversa del elemento a módulo m.*

Demostración. Sea $\frac{P_{n-1}}{Q_{n-1}}\ y\ \frac{P_n}{Q_n}$ las dos últimas reducidas del número $m\ /\ a$, entonces $m = P_n, a = Q_n$ y según el corolario 11.3.5,

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)n}{Q_{n-1}\,Q_n}.$$

Por consiguiente,

$$\frac{m}{a} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)n}{Q_{n-1}\,Q_n}, \qquad Q_{n-1}m - aP_{n-1} = (-1)n\ y$$

$a(-1)n - 1\ P_{n-1} \equiv 1(modulo\ m\ )$. ■

Ejemplo. Busque el número inverso del número 79 del módulo $m = 273$.

Descomponga el número $\frac{273}{79}$ en fracción continua, entonces

$\frac{273}{79} = |3; 2,5,7|$.

Calcule los numeradores reducidos del número $\frac{273}{79}$ siguiendo el esquema

k		1	2	3	4
$q_{\Re}$		3	2	5	7
$p_{\Re}$	1	3	7	38	273

$p_3 = 38$ Es el numerador antepenúltimo reducido del número 273/79. Por tanto, el número $(-1)^3 P_3 = -38$ es la inversa del número 79, es decir, $79(-38) \equiv 1(módulo\ 273)$.

Función de Euler. El número de enteros positivos no superior n y primero con él se denota así $\varphi(n)$; la función numérica φ define sobre el conjunto de todos los enteros positivos se denomina *función de Euler (o denominada indicatriz de Euler).* Se observa fácilmente que $\varphi(n)$ es igual al número de enteros no negativos inferiores en n y primos con él.

Ejemplo: $\varphi(1) = 1,\ \varphi(2) = 1,\quad \varphi(6) = 2,\ \varphi(5) \simeq 4,\ \varphi(12) = 4.$

La función numérica f se denomina *multiplicativa* si para todo enteros positivos $a\ y\ b$ primos entre ellos, se tiene la igualdad $f(ab) = f(a)f(b)$.

TEOREMA 3.9 *La función de Euler φ es multiplicativa.*

Demostración. Sean $a\ y\ b$ enteros positivos primos entre ellos. Considérese el conjunto M de todos los enteros no negativos inferiores en ab. Según el TEOREMA de la división con resto, cada número M se puede representar de manera única bajo la forma de $bq + r, donde\ r \in \{0,1, \dots, b-1\}, q \in \{0,1, \dots, a-1\}$. El número $bq + r$ es primo con a si y sólo si $(b, r) = 1$. Existe $\varphi(b)$ de tales r. Sea $r_1, b + r_1, 2b + r_1, \dots, b\ (a-1) + r_1$ que forman un sistema completo de residuos de módulo a. Así, existe entre estos números exactamente $\varphi(a)$ números primos con a. Entonces, en cada numero r_1 primo con b están asociadas exactamente $\varphi(a)$ números de la forma $bq + r_1$ primos con a y por consiguiente, con ab. También el número de números que pertenecen a M y primos con abes igual en $\varphi(a)\ \varphi(b)$, es decir, $\varphi(ab) = \varphi(a)\ \varphi(b)$.

TEOREMA 3.10. *Si* $n = \prod_{p|n} p^{\alpha_p}$ *es una descomposición canónica del número natural n, entonces*

(1) $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{P}\right)$.

Demostración. Dado que la función φ es multiplicativa, para el cálculo de $\varphi(n)$, se es capaz de calcular esta función por una potencia del número primo P. El número de enteros no negativos inferiores en $P^{\propto}$ y no primos con $P^{\propto}$ es $p^{\propto-1}$, ya que solo los números $Kp, 0 \le k < p^{\propto-1}$ no son primos con $P^{\propto}$. También el número de números inferiores en $P^{\propto}$ y primos con $P^{\propto}$ vale $P^{\propto} - p^{\propto-1}$, es decir,

(2). $\varphi(p^{\propto}) = P^{\propto}\left(1 - \frac{1}{P}\right)$.

Dado que $n = \prod_{p|n} p^{\propto p}$ y la función φ es multiplicativa, tenemos

(3) $\varphi(n) = \prod_{p|n}\varphi(P^{\propto p})$.

DE (2) Y (3) se deduce que

$$\varphi(n) = \prod_{p|n} P^{\propto p}\left(1 - \frac{1}{P}\right) = \prod_{p|n} P^{\propto p}\prod_{p|n}\left(1 - \frac{1}{P}\right) = n\prod_{p|n}\left(1 - \frac{1}{P}\right),$$

y, a continuación, la formula (1) se verifica. □

Ejemplo: $\varphi(30) = 30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$

TEOREMA 3.11. La suma de números $\varphi(d)$ que sigue todos los divisores naturales d del número n es n, es decir,

$$\sum_{d|n} \varphi(d) = n.$$

Demostración. Si $n = \prod i\ P_i^{\propto_i}$ es una descomposición canónica de n, entonces

$\sum_{d|n} \varphi(d) = \prod i\left(1 + \varphi(p_i) + ({p_i}^2) + \cdots + \varphi\left({p_i}^{\propto_i}\right)\right)$,

al abrir los paréntesis, se obtiene la suma de todos los valores de $\varphi(d)$. Luego,

$\sum_{d|n} \varphi(d) = \prod i\ (1 + (p_i - 1) + ({p_i}^2 - p_i) + \cdots ({p_i}^{\propto_i} - {p_i}^{\propto_i - 1}) = \prod i {P_i}^{\propto_i} = n$, Es decir,

$$\sum_{d|n} \varphi(d) = n.$$

TEOREMA de Euler y de Fermat. En teoría de congruencias una función muy importante es el TEOREMA de Euler.

TEOREMA DE EULER. *Si un entero a es un número primo con m, entonces*

(1) $a^{\varphi(m)} \equiv 1(modulo\ m)$.

Demostración. Sea

(2) $a_1, a_2, \ldots, a_{\varphi(m)}$

un sistema residual reducido de módulo m, entonces, según la proposición 3.4,

(3) $aa_1\ \ aa_2, \ldots, aa_{\varphi(m)}$

es igual. También el producto de números (3) es congruente al producto de números (2), es decir,

(4) $a^{\varphi(m)} a_1 a_2 \ldots a_{\varphi(m)} \equiv a_1 a_2 \ldots a_{\varphi(m)}\ (\acute{o}m)$.

El producto $a_1 a_2 \ldots a_{\varphi(m)}$ es primo con m. También, según la propiedad 1.6, ambas partes de la congruencia (4) se adaptan a una división por ese producto y se tiene $a^{\varphi(m)} \equiv 1\ (m\acute{o}dulo\ m)$. □

TEOREMA DE FERMAT. *Si un número entero a no es divisible por el número primo p, entonces,* $a^{p-1} \equiv 1(m\acute{o}dulo\ P)$.

Este TEOREMA es un caso particular del TEOREMA anterior en el caso donde $m = P$. Se enuncia seguido el TEOREMA de Fermat de manera diferente.

SEGUNDO ENUNCIADO DEL TEOREMA DE FERMAT. *Si p es primo y a un entero cualquiera, entonces,* $a^p \equiv a(m\acute{o}dulo\ p)$.

Ejercicios

1. A partir de la igualdad $a^p = (1 + 1 \ldots + 1)p$, demostrar que para todo a natural y p primo la congruencia $a^p \equiv a(m\acute{o}dulo\ p)$ se satisface.
2. Demostrar que el número de fracciones reducidas positivas que tenga por denominadores uno de los números siguientes 1, 2,…, n y no supere la unidad valido $\varphi(1) + \varphi(2) + \cdots + \varphi(n)$.
3. Demostrar que para todo $n > 1$ la suma de residuos m módulo n que tienen en el intervalo $1 \leq m < n$ es igual en $\frac{1}{2} n\varphi(n)$.
4. Mostrar con ejemplos que la congruencia $a^m \equiv a(m\acute{o}dulo\ m)$, donde m es primo, no se puede verificar por un m compuesto.

5. Demostrar que si $a^{n-1} \equiv 1\ (módulo\ n)$ y $^{ad} \not\equiv 1$ para todo divisor positivo d del número $(n-1)$, entonces, n es primo.
6. ¿Cuantos números naturales inferiores al número 234 000 000 y primos con él?

§4. Congruencias de primer grado.
Congruencias de grados superiores que sigue un módulo simple

Grado y número de soluciones de la congruencia . La congruencia de la forma

(1) $a_n x^n + \ldots + a_1 x + a_0 \equiv 0\ (mod\ m)$,

donde $a_1, \ldots, a_n$ son los enteros, se denomina *congruencia algebraica.*
El número n es denominado grado de la congruencia (1) si a_n, no es divisible por m.

Si el número a satisface a la congruencia (1), entonces todo número b congruente en a módulo m sastiface igualmente la congruencia (1); estas dos soluciones se consideran como idénticas.

DEFINICIÓN. Se denomina *número de soluciones de la congruencia módulo* m al número de soluciones de esta congruencia en el sentido de un sistema completo cualquiera de residuo de módulo m.

Ejemplos.1. La congruencia $3x^2 - 7 \equiv 0$(mod 4) entre los números 0, 1, 2,3 del sistema completo, de residuos de módulo 4 se cumple para dos números: $x = 1$ y $x - 3$. Entonces la congruencia tiene dos soluciones: $x \equiv 1$(mod 4) y $x \equiv 3$ (mod 4).

2. En la congruencia $x^2 \equiv 1$(mod 8),entre los números 0,1,2,3,4,,5,6,7 del sistema completo de residuos módulo 8 cumplieron a cuatro números :1,3,5,7.Es decir que la congruencia tiene cuatro soluciones:

$x \equiv 1$(Módulo 8), $x \equiv 3$(mod 8), $x \equiv 5$ (mod 8), $x \equiv 7$(mod 8).

Congruencia de primer grado. Búsquese las condiciones de resolubilidad de la congruencia de primer grado.
TEOREMA 4.1. Si $(a, m) = 1$, *entonces la congruencia*

(1)$ax \equiv b$(mod m)

admite una y solamente una solución.

Demostración. Por hipótesis el número a es primo con m. Según el TEOREMA 3.5 existe un entero a' inverso de a módulo m, es decir $a'a \equiv 1(\ mod\ m)$.Multiplíquese los dos miembros de (1) por a' , se tiene

(2)$x \equiv a'b(\ mod\ m)$

Por tanto, la congruencia (1) admite una solución o más. Además, (2) es una solución de la congruencia (1), por que

$a(a'b) \equiv (aa')b \equiv (\ mod\ m)$

También, la clase residual $a'bmodm$ es la única solución de la congruencia (1).□

TEOREMA 4.2. *Sea* $(a, m) = d$. *La congruencia*

(1) $ax \equiv b\ (modm)$

es resoluble si y sólo si $d \mid b$.*Si* $d \mid b$, *la congruencia (1) posee a manera de serie de soluciones exactamente* d *clases residuales de módulo* m *que costituyen una clase residual común de módulo* m/d.

Demostración .Sea $(a, m) = d > 1$. Si la congruencia (1) tiene por solución x_1 entonces $ax_1 - b = km$ donde k es un entero .Dado que $(a, m) = d$, se deduce que d divide a b.

Admítase ahora que b es divisible por d y demuéstrese que la congruencia (1) tiene d soluciones .Sean $b = b_1 d, a = a_1 dym = m_1 d$. La congruencia (1) es equipotente a la congruencia (2)$a_1 x \equiv b_1 (mod\ m_1)$.
Según el TEOREMA 4.1 , la congruencia (2) posee una única solución $a_1^{'} b_1\ mod\ m_1$, donde $a_1^{'}$ es un número inverso de $a_1$módulo m_1.Sea $x_0 = a_1^{'} b_1$.La clase residual $x_0 \text{mod} m_1$ se separa en d clases residuales de módulo m siguientes:

(3)$x_0 \text{mod} m, (x_{0+} m_1) mod\ m, (x_{0+} 2m_1) mod\ m, \ldots, x_0 + (d-1)m,)\ mod\ m$

Se constata sin duda que las clases residuales (3) son las clases residuales de módulo m distinta. También, la congruencia (2) posee una serie de soluciones de clases residuales (3), es decir exactamente d clases residuales de módulo m que constituye una clase residual única módulo $m\ /\ d$.□

Nótese que la colección de las soluciones (3) de la congruencia (1) es una del grupo aditivo $\mathcal{G}$ de las clases residuales módulo m que siguen los sub-grupos $\frac{m}{d}.\mathcal{G}$. Recíprocamente: Toda clase que sigue el subgrupo $\frac{m}{d}\mathcal{G}$ del grupo$\mathcal{G}$ puede tomarse por un conjunto de soluciones de alguna congruencia lineal módulo$m$.

Congruencia de grados superiores que sigue un módulo simple

Pásese al problema de números de soluciones que admite una congruencia de grado n que sigue un módulo simple.

TEOREMA 4.3. *La congruencia*

(1)$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 (mod\ p)$

De grado n que sigue un módulo simple p admite n soluciones o más.

Demostración (se efectúa por inducción en n). Si $n = 0$, la congruencia es de la forma $a_0 \equiv 0 (mod\ p)$, donde $p + a_0$; en este caso la congruencia tiene cero soluciones. Supóngase que la congruencia (1) es de grado $n > 0$. Si la congruencia admite soluciones, entonces para algún entero x_1 , se tiene

(2) $a_n x_1^n + \ldots + a_1 x_1 + a_0 \equiv 0 (mod\ p)$

Sustráigase esta congruencia de (1).En este caso, la diferencia entre los términos de grado k es de la forma

$$a_k \left(x^k - x_1^k\right) = a_k (x - x_1)\left(x^{k-1} + x_1 x^{k-2} + x_1^{k-1}\right)$$

con $k = 1, \ldots, n$; cada diferencia contiene un factor lineal $(x - x_1)$.Por tanto, se puede escribir finalmente la diferencia de la manera siguiente:

(3) $(x - x_1) b_{n-1} x^{n-1} + \ldots + b_0) \equiv 0 (mod\ p)$,

donde $b_0, \ldots, b_{n-1}$ son enteros $b_{n-1} = a_n$. Cualquier otra solución de la congruencia (1) dígase, $x_2$será la solución de la congruencia

(4) $b_{n-1} x^{n-1} + \ldots + b_0 \equiv 0\ (mod\ p)$

De hecho, dado que $x_2 \not\equiv x_1 (mod\ p)$ y el módulo p es simple, de la congruencia

$$(x_2 - x_1)(b_{n-1} x_2^{n-1} + \ldots + b_0) \equiv 0 (mod\ p)$$

a menos que

$b_{n-1}x^{n-1}+\ .\ .\ .+b_0 \equiv 0(mod\ p)$.

Como el grado de la congruencia *(4)* vale $n-1$. Siguiendo la hipótesis de inducción, la congruencia (4) admite $n-1$ soluciones o más.

Por lo tanto, la congruencia de partida (1) admite n soluciones o mas.□

COROLARIO 4.4. *Si la congruencia* $a_n x^n+\ .\ .\ .+a_1 x+a_0 \equiv 0(mod\ p)$ *admite más de* n *soluciones, todos sus coeficientes son divisibles por p.*

PROPOSICIÓN 4.5. *Si p es primo, la congruencia* $x^{p-1}-1 \equiv 0(mod\ p)$ *admite exactamente* $p-1$ *soluciones.*

Esta proposición se deriva directamente del TEOREMA de Fermat y todos los números no divisible por p satisfacen a la congruencia; sus soluciones son los números 1, 2, ,$p-1$.

TEOREMA DE WILSON .*Si p es primo entonces*

(1) $(p-1)\,!+1 \equiv 0(mod\ p)$.

Demostración. Si $p=2$ el TEOREMA es aparentemente verdadero. Sea $p>2$.Considérese la congruencia

(2) $(x-1)(x-2).\ .\ .(x-(p-1))-(x^{p-1}-1) \equiv 0(modp)$.

Su grado es inferior a $p-1$ pero esta congruencia posee $p-1$ soluciones :1, 2, . . . ,$p-1$. También, según el corolario 4.4, todos los coeficientes de la congruencia (2) son divisibles por p.En particular, el último coeficiente igual a $p-1!+1$ es divisible por p.□

TEOREMA 4.6 *Si p es primo y d es un divisor natural del conjunto* $p-1$*, la congruencia*

(1) $x^d-1 \equiv 0(mod\ p)$

entonces tiene exactamente d soluciones

Demostración .Sea d un divisor cualquiera de $p-1, p-1=kd$. Entonces la congruencia

(2) $x^{p-1}-1 \equiv 0(mod\ p)$

puede escribirse bajo la forma

(3) $x^d-1(x^{d(k-1)}+x^{d(k-2)}+\ .\ .\ .+x^d+1 \equiv 0(mod\ p)$

Según la proposición 4.5, la congruencia (2) posee $p-1$ soluciones :1, 2, . . . ,$p-1$. Cada solución de la congruencia (2) debe verificar una de las congruencias:

(1) $x^d-1 \equiv 0(mod\ p)$

(4) $x^{d(k-1)}+.\ .\ .+x^d+1 \equiv 0(mod\ p)$

Según el TEOREMA 4.3 la congruencia (4) admite $d(k-1)=p-1-d$ soluciones o más. Es decir, la congruencia (1) debe poseer al menos d soluciones. Por lo tanto, en razón a la proposición 4.5, la congruencia (3) tiene exactamente d soluciones.□

Ejercicios

1. Demostrar que si el número natural $m>1$, la congruencia 1.2.3. . . . . .$(m-1) \equiv -1(mod\ m)$ entonces se cumple si y sólo si m es primo.
2. Buscar las soluciones de la congruencia $ax \equiv 1(mod\ 7) para\ a=2,3,4,5,6.$

3. Buscar el número múltiplo de 7 y proporcionarle menos 1 después divirlo por 2, 3, 4, 5, 6.
4. Demostrar que la congruencia $x^2 + 1 = 0(mod\ p)$ para $p = 4n + 1$ primo. Se cumple para el número (2n)!
5. Resolver las congruencias
6. $x^2 \equiv -1(mod\ 65)$; $x^2 \equiv -2(mod\ 33)$

§ 5. Raíces primitivas e índices

Orden de números y de la clase residual que sigue un módulo. Sea a un número primo con m .*Se* denomina *orden de número a módulo m* al menor entero positivo d de manera que $a^d \equiv 1(mod\ m)$. Si $b \equiv a(mod\ m)$, posee el mismo orden de módulo m que a. Así, todos los elementos de la clase residual $a\ mod\ m$ son de orden d; el número d se denomina *orden de la clase residual* a módulo $m = d$ *y se denota* $\vartheta(a\ mod\ m)$.

PROPOSICIÓN *5.1. Si* $\vartheta(a\ mod\ m) = d$ *entonces los números* $a, a^2, \ldots\ldots a^d$ *no son congruentes en ambos módulo* m.

Demostración. Si $a^s \equiv a^k(mod\ m)$, donde $k < s, k, s \in \{1,2,\ldots,d\}$, entonces $a^{s-k} \equiv 1(mod\ m)$, lo que es contradictorio con la hipótesis, puesto que $0 < s - k < d$.□

PROPOCISIÓN 5.2. *Sea* $\vartheta\ (a\ mod\ m) = d$ *y* n *entero no negativo. La congruencia* $a^n \equiv 1(mod\ m)$ *se confirma si y sólo si* n *es divisible por* d.

Demostración. Muéstrese primero, que se deduce a partir de $a^n \equiv 1(mod\ m)$ que n es divisible por d. Según el TEOREMA de la división con resta, existe para $n\ y\ d$ los números naturales q y r tales que

(1) $n = dq + r$, $0 \le r < d$.

Demuéstrese que $r = 0$. En razón a (1) y de la condición $a^d \equiv 1(mod\ m)$, se tiene

$$a^n \equiv a^{dq}a^r \equiv \left(a^d\right)q_{a^r} \equiv a^r \equiv 1(mod\ m)$$

Dado que, por hipótesis $a^r \not\equiv 1(mod\ m)$, si $0 < r < d$, la congruencia $a^r \equiv 1(mod\ m)$ es posible solo para $r = 0$. Por lo tanto, n es divisible por d. Supóngase ahora que n es divisible por d, $n = dk$ para cierto k. Entonces

$a^n \equiv a^{dk} \equiv \left(a^d\right) \equiv 1(mod\ m)$, es decir $a^n \equiv 1(mod\ m)$.□

PROPOCISIÓN 5.3. *SI* $\vartheta\ (a\ mod\ m) = d$ *, entonces* $\varphi(m)$ *es divisible por* d.

Demostración. Conforme a la proposición 5.2 de $a^{\varphi(m)} \equiv 1(mod\ m)$ y de la condición $\vartheta(a\ mod\ m) = d$ se deduce que $\varphi(m)$ es divisible por d.□

PROPOCISIÓN 5.4 *Sea* $\vartheta\ (a\ mod\ m) = d$ *la congruencia* $a^s \equiv a^{\Re}(mod\ m)$ *procede si y sólo si* $k \equiv s(mod\ d)$.

Demostración. Si

(1) $a^R \equiv a^s(mod\ m)$ $k \ge s$,

entonces

(2) $a^{R-s} \equiv 1(mod\ m)$

y, como resultado, conforme a la proposición 5.2, $k - s$ es divisible por d , es decir

(3) $k \equiv s\ (mod\ d)$

Recíprocamente: de (3) se derivan (2) y (1).□

PROPOSICIÓN 5.5. *Sean a, b números primos con m si los números $\vartheta\ (a\ mod\ \ m)$ y $\vartheta(b\ mod\ m)$ son primos entre ellos, entonces*

$\vartheta(ab\ mod\ m) = \vartheta(a\ mod\ \ m).\vartheta(b\ mod\ m).$

Demostración .Sean $\vartheta(a) = d, \vartheta(b) = e$ y $\vartheta(ab) = f$. Demuéstrese que f es divisible por d. Dado que $b^e \equiv 1(mod\ m)\ entonces\ \ a^e \equiv a^e b^e \equiv (ab)^e (mod\ m)$ y $a^{ef} \equiv (ab)^{ef} \equiv \left((ab)^f\right)^{\mathrm{e}} \equiv 1\ (mod\ m)$. A partir de $a^{ef} \equiv 1(mod\ m)$, conforme a la proposición 5.2 se deduce que ef es divisible por d. Dado que por hipótesis $(d, e) = 1, f$ es divisible por d. Se obtiene lo mismo que f es divisible por e. Por lo tanto, f es divisible por de.

Por otra parte $(ab)^{de} \equiv \left(a^d\right)^{\mathrm{e}} (b^e)^{\mathrm{d}} \equiv 1(mod\ m)$. Según la proposición 5.2 se deduce que de es divisible por f. Por lo tanto, $f = de$.□

PROPOSICIÓN 5.6. *Si $\vartheta\ (a\ mod\ m\ ) = n$ y d es un divisor natural del número n , entonces $\vartheta\left(a^d\ mod\ m\right) = n/d$.*

Demostración .Sea $\vartheta\left(a^d\ mod\ m\right) = f$. Por hipótesis $a^n \equiv (a^d)^{\mathrm{n}}/^{\mathrm{d}} \equiv 1(mod\ m)$. Según la proposición 5.2, se deduce que n/d es divisible por f, es decir $n/d = kf, n = kfd$ para cierto número natural k. Por lo tanto, $a^{fd} \equiv (a^d)^{\mathrm{f}} \equiv 1(mod\ m)$.Se deduce que fd es divisible por n. Por lo tanto, $k = 1, n = fd\ y\ f = n/d$.□

PROPOSICIÓN 5.7. Si $\vartheta\ (a\ mod\ m\ ) = n\ \ y(k, n) = d$ entonces $\vartheta\left(a^k\ mod\ m\right) = n/d$

Demostración. Sean $\vartheta\left(a^k mod\ m\right) = f, k = k_1 d, n = n_1 d$. De la hipótesis se deduce que $(a^k)^{\mathrm{n}}\ /\ ^{\mathrm{d}} \equiv (a^n)^{k/d} \equiv 1(mod\ m)$.

Por lo tanto, el número $n/d = n_1$ es divisible por f. Por otra parte, $(a^k)^{\mathrm{f}} \equiv a^{kf} \equiv 1(mod\ m)$. Según la proposición 5.2, se deduce que kf es divisible por n. Por lo tanto, $k_1 f$ es divisible por n_1; dado que $(k_1, n_1) = 1, f$ por lo tanto es divisible por, n_1; por consiguiente, $f = n_1 = n/d$.□

PROPOSICIÓN 5.8. *Si $\vartheta\ (a\ mod\ m\ ) = n\ \ y(k, n) = 1$, entonces $\vartheta\left(a^k\ mod\ m\right) = n.$*

Esta proposición se deriva directamente de la anterior.

Raíces primitivas que sigue un módulo simple. Para describir un grupo de residuos multiplicativos siguiendo un módulo simple, es necesario proceder al estudio de los números cuyo orden es el mayor que sigue este módulo.

TEOREMA 5.9*. Sea p un número primo y d un divisor natural del número $p - 1$. En un sistema reducido de residuos de módulos p existe exactamente $\varphi(d)$número de orden d.*

Demostración. Sea B el sistema reducido de residuos de módulo p. Sea d cierto divisor natural del número $p - 1$.

Nótese $\psi(d)$ el número de elementos de B cuyo orden es d . Supóngase que existe al menos un elemento $a \in B$ cuyo orden es p, es decir $\psi(d) > 0$. Entonces, a, a^2 , . . . a^d son soluciones de módulo p distintas de la congruencia

(1) $x^d \equiv 1(modp)$

y, según el TEOREMA 4.6, no hay otras soluciones .Como resultado, todo los residuos de orden d deben pertenecer al conjunto

$M = \{a, a^2,\ \ldots,\ a^d\}.$

Según las proposiciones 5.7 y 5.8 el número a^kes de orden d si y sólo si $(d, k) = 1$. Se deduce que $\psi(d) = \varphi(d)$ en caso que exista al menos un elemento de orden d. Así

(2) $\psi(d) \leq \varphi(d)$ para todo divisor d del número $p - 1$.

Cada residuo que posee un orden d, divisor de $p-1$, se tiene

$$\sum_{d\ 1(p-1)} \psi(d) = p-1$$

Por otra parte, según el TEOREMA 3.11,

$$\sum_{d\ 1(p-1)} \varphi(d) = p-1$$

Por lo tanto

(3)
$$\sum_{d\ 1(p-1)} (\varphi(d) - \psi(d)) = 0\ .$$

Tomando como base (2) y (3) se concluye que $\psi(d) = \varphi(d)$ para todo divisor natural d del número $p-1$.□

Si el residuo a módulo m es de orden $\varphi(m)$, entonces se denomina *a raíz primitiva módulo m.*

TEOREMA 5.10. *Un grupo de residuos de módulo p primo con el módulo es cíclico .El número de raíces primitivas módulo p vale $\varphi\ (p-1)$.*

Este TEOREMA se deriva directamente del TEOREMA anterior según el cual existe $\varphi\ (p-1)$ generadores del grupo de residuos primos con p.

Si g es la raíz primitiva módulo p los $p-1$ potencias

(1) $g, g^2, \ \ldots\ , g^{p-1}$

Son entonces no son congruentes al módulo p.Por lo tanto, la proposición siguiente es verdadera.

PROPOSICIÓN 5.11. *Si g es la raíz primitiva de módulo p los $p-1$ potencias $g, g^2, \ \ldots\ , g^{p-1}$ entonces constituyen un sistema reducido de residuos de módulo p.*

Las raíces primitivas no existen para todo módulo m pero sólo para $m = 2,4, p^k, 2p^k$(siendo p un número primo impar).

Ejemplo. Sea $p = 13$. Búsquese las raíces primitivas que sigue este módulo.

El número $p-1 = 12$posee 6 divisores naturales: 1, 2, 3, 4, 6,12:

$$\varphi(1) = 1\ ,\ \varphi(2) = 1,\ \varphi(3) = 2\ ,\ \varphi(4) = 2, \varphi\ (6) = 2,\ \varphi(12) = 4.$$

Los números 2, 6, 7, 11 son raíces primitivas de módulo 13. El número 12 tiene orden 2; el número 3 el orden 3; los número 5,8 el orden 4; los números 4,10 el orden 6, el número 1 el orden 1.

Índices que sigue un módulo simple. Sea$g$ una raíz primitiva módulo p. Entonces, los números

(1) $\mathrm{g}, \mathrm{g}^2, \ \ldots\ , \mathrm{g}^{p-1}$

Forman un sistema reducido de residuos de módulo p. También todo número a es primo con p y es congruente con uno y solamente uno de los números de la serie (1).

Si $a \equiv \mathrm{g}^k (mod\ p)$, entonces k se *llama índice del conjunto a módulo p* que afecta la base g y que se designa por el símbolo $ind\ a\ \ o\ ind_{\mathrm{g}} a$.

Si k' es otro número por el cual $a \equiv \mathrm{g}^{k'} (mod\ p)$, entonces $\mathrm{g}^k \equiv \mathrm{g}^{k'} (mod\ p)$ y, según la proposición 5.4 $k \equiv k' (mod(\ p-1))$.

Así, el conjunto de índices de un número a dado, forman una clase residual módulo $p-1$. Por definición del índice, $a \equiv b (mod\ p)$implica $ind\ a \equiv ind\ b\ (mod\ p-1)$.

Ejemplo. Sea $p = 13$. El número 2 es la raíz primitiva módulo 13. Los índices de los números 1, 2 , . ,12 que afecta la base $\mathrm{g} = 2$ son:

a	1	2	3	4	5	6	7	8	9	10	11	12
$ind\ a$	0	1	4	2	9	5	11	3	8	19	7	6

Con la ayuda de este cuadro, dada la base del número a, se obtiene su índice de módulo 13. Conociendo el índice, el tabla que sigue permite obtener el número correspondiente:

$ind\ a$	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

Mediante índices se está en capacidad de reducir una multiplicación de módulo p en una adición de módulo $p-1$, de manera análoga el proceso que permite con la ayuda de logaritmos de reducir una multiplicación banal de números en una adición .

TEOREMA 5.12. *Si los números a, b son primos con p y n es un número natural cualquiera, entonces*

(1) $ind\ ab \equiv ind\ a + ind\ b\ (mod\ p-1)$

$ind\ a^n \equiv n\ ind\ a\ (mod\ p-1)$.

Demostración. Por definición los índices de los números $a\ y\ b$ se tiene :

$a \equiv \mathrm{g}^{ind\ a} (mod\ p)$, $\qquad b \equiv \mathrm{g}^{ind\ b} (mod\ p)$,

de ahí, se obtiene el producto

$ab \equiv \mathrm{g}^{ind[a+ind\ b}(mod\ p)$.

Por lo tanto, $ind\ a + ind\ b$ es uno de los índices del producto ab , es decir

$ind\ ab \equiv ind\ a + ind\ b\ (mod\ p-1)$.

De la congruencia $a \equiv \mathrm{g}^{ind\ a} (mod\ p)$ se deduce que

$a^n \equiv \mathrm{g}^{n\ ind\ a} (mod\ p)$;

También $n\ ind\ a$ es uno de los índices de la potencia a^n, es decir

$ind\ a^n \equiv n\ ind\ a (mod\ p-1)$.□

Ejemplos. 1. Sean $p = 13, a = 8\ , b = 6$; entonces $ind\ 8 = 9, ind\ 6 = 8\ , ind\ 8.6 \equiv 9 + 8 \equiv 5 (mod\ 12)$.

2. Resolver la congruencia $6x \equiv 7(mod\ 13)$.

La congruencia dada es equivalente a:

$$ind\ 6 + ind\ x = ind\ 7(mod\ 12) \text{ o } ind\ x \equiv ind\ 7 - ind6 = 11 - 5 = 6(mod\ 12).$$

Se deduce que $x \equiv 12(mod\ 13)$.

TEOREMA 5.12. *Sea $\mathcal{G}_p$ un grupo multiplicativo de clase residual, elementos primarios con p y C un grupo aditivo de la clase residual del módulo $p-1$. La función $a\ mod\ p \longmapsto ind\ a\ (mod\ p-1)$, que asocia a cada elemento a del grupo $\mathcal{G}_p$ el elemento $ind\ a$ del grupo C es un isomorfismo del grupo $\mathcal{G}_p$ en el grupo C.*

Demostración. Por definición de índice, la correspondencia $a\ mod\ p \underset{\varphi}{\rightarrow} ind\ a\ (mod\ p-1)$, es biyectiva .Por otra parte, en el grupo $\mathcal{G}_p$ se respecta a la operación de multiplicación, ya que de la congruencia

$$ind\ ab \equiv ind\ a + ind\ b\ (mod\ p-1)$$

Se deduce que

$$[ind\ ab] = [ind\ a] + [ind\ p].$$

Por lo tanto, φ es un isomorfismo del grupo $\mathcal{G}_p$ en el grupo C.□

En aritmética modular, el fundamento de la teoría de logaritmos es un isomorfismo del grupo multiplicativo de los números reales positivos y del grupo aditivo de todos los números reales. El TEOREMA demostrado, que constituye el fundamento de la teoría de índices permite comprender, porqué la teoría de logaritmos (de la aritmética modular) se parece a la teoría de índices (siguiendo un módulo simple).

Congruencias binomiales . Se denomina *congruencia binomial* a la congruencia de la forma

(1) $ax^n \equiv b(modp)$,

donde el exponente es positivo. Si p es primo, la congruencia (1) es equivalente a la congruencia

(2) $n\xi \equiv ind\ b - ind\ a(mod\ p-1), donde\ \xi = ind\ x.$

Para que la congruencia (2) sea resoluble es necesario y basta que el número $d = (n, p-1)$ divida la diferencia $ind\ b - ind\ a$. Si esta condición se cumple, la congruencia (2) admite d soluciones de módulo $p-1$; por lo tanto, la congruencia (1) posee exactamente d soluciones de módulo p.

Ejemplo. Resuélvase la congruencia

(3) $6x^8 \equiv 5(mod 13)$.

La congruencia (2) toma en este caso la forma

$$8\xi \equiv ind\ 5 - ind\ 6(mod\ 12); \quad donde\ 8\xi \equiv 4(mod\ 12)$$

Esta última congruencia es compatible, dado que (8,12) dividen a 4 y admite las cuatro soluciones siguientes:

$$\xi \equiv 2, 5, 8, 11(mod 12); \quad ind\ x \equiv 2, 5, 8, 11(mod\ 12).$$

Por lo tanto, la congruencia (3) posee cuatro soluciones:

$x \equiv 4, 6, 9, 7 (mod\ 13)$.

La congruencia binomial (1) se puede reducir a una más simple multiplicando los dos miembros de la congruencia por el número a', inversa de a módulo $p, a', a \equiv 1 (mod\ p)$. La multiplicación efectuada se obtiene $x^n \equiv a'b (mod\ p)$. Así, toda congruencia binomial se puede reducir a la forma más simple:

$x^m \equiv c (mod\ p)$.

DEFINICIÓN. El número a *se denomina k-naria residuo de módulo* m si la congruencia $x^k \equiv a (mod\ m)$ admite al menos una solución.

Sea p un número primo y $\bar{k} = (k, p-1)$.

TEOREMA 5.13. *Para todo residuo a que sigue un módulo simple p las afirmaciones siguientes son equivalentes:*

(α) a *es un k-naria residuo de módulo* p;

(β) $a^{\frac{p-1}{\bar{k}}} \equiv 1 (mod\ p)$;

(γ) *el orden de la clase residual a módulo p es un divisor del número* $\frac{p-1}{\bar{k}}$, *es decir* $\vartheta (a\ mod\ p) \mid ((p-1)/\bar{k})$;

(δ) ind a es un múltiplo de $\bar{k}$.

Demostración. $(\alpha) \rightarrow (\beta)$. Sea a el *k-n*aria residuo; entonces, existe un residuo x_0 primo con p que verifica la congruencia $x_0^k \equiv a (mod\ p)$.Por lo tanto,

$$a^{\frac{p-1}{\bar{k}}} \equiv (x_0^k)^{\frac{p-1}{\bar{k}}} \equiv \left(x_0^{k/\bar{k}}\right)^{p-1} \equiv 1 (mod\ p),$$

es decir que (β) se verifica;

$\beta) \rightarrow (\gamma)$. Según la proposición 5.2 de la congruencia (β) se deduce (γ);

$(\gamma) \rightarrow (\delta)$. De la condición (γ) se deduce que

(1) $a^{\frac{p-1}{\bar{k}}} \equiv 1 (mod\ p)$.

Sea g una raíz primitiva de módulo p . Entonces, $a = \mathrm{g}^{ind\ a}$ y conforme a (1),

$$(\mathrm{g}^{ind\ a})^{\frac{p-1}{\bar{k}}} \equiv (\mathrm{g}^{ind\ a.\frac{p-1}{\bar{k}}} \equiv 1 (mod\ p).$$

Por lo tanto, según la proposición 5.2,

$$(ind\ a^{\frac{p-1}{\bar{k}}} \equiv 0 (mod\ p-1);$$

y, mediante, $\bar{k} \mid ind\ a$, es decir que cumple (δ).

$(\delta) \rightarrow (\alpha)$. Considérese la congruencia

$k\xi \equiv ind\ a(mod\ p-1)$

dado que $\bar{k} = (k, p-1)/ind\ a$, la congruencia admite una solución. Sea ξ_0 la solución de esta congruencia , $k\xi_0 \equiv ind\ a\ x(mod\ p-1)$. Entonces, $g^{k\xi_0} \equiv g^{ind\ a}(mod\ p)$, por lo tanto, $(g^{\xi_0})^k \equiv a(mod\ p)$, es decir a es la $k-naria$ residuo de módulo p.
Así, $(\delta) \rightarrow (\alpha)$.□

Ejercicios

1. Componer la tabla de los índices módulo 19 de base 2.
2. Componer la tabla de los índices módulo 29 de base 10.
3. Buscar las raíces primitivas de los números 41 y 49.
4. Sea p un número primo impar y $n > 1$. Mostrar que existe exactamente $(p-1)$. $\varphi(p-1)$ raices primitivas diferentes del número p^n no congruente de módulo p^2.
5. Si p es un número primo impar $n > 1$, existe exactamente $\varphi(\varphi(p^n))$ raíces primitivas diferentes del número, p^n.
6. Mostrar que si p es un número primo impar y $n > 1$existe exactamente $\varphi(\varphi(p^n))$ raíces primitivas diferentes del número $2p^n$.
7. Buscar el índice del número (-1) siguiendo un módulo simple impar p, siendo la base cualquiera.
8. Mostrar que para un número primo de la forma $2^n + 1$ con $n > 3$, el número 3 es una raíz primitiva.
9. Mostrar que si p es un número primo de la forma $4k + 1$ y g la raíz primitiva de módulo $p, p - g$ también es una raíz primitiva módulo p.

§ 6. Conversión de una fracción ordinaria en fracción sistemática y apreciación de la longitud del período de una fracción sistemática

Una fracción periódica m-naria

$$m^h(b_1 m^{l-1} + \ldots + b_l + \frac{a_1}{m} + \ldots \frac{a_k}{m^k} + \frac{a_1}{m^{k+1}} + \ldots + \frac{a_k}{m^{2k}} + \ldots)$$

Se escribe de manera abreviada de la forma

(*) $m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k})$

$a_1 \ldots a_k$ en este caso se denomina *periodo de la fracción y* $b_1 \ldots b_l$ *pre-periodo de la fracción.* El número k es la *longitud del periodo y* el número l *la longitud del pre-periodo*

La fracción periódica m-naria (*) se denomina n*ormada* si se cumplen las condiciones:

$(\alpha) a_k \neq b_l$;
(β) el periodo $a_1 \ldots a_k$ posee la más mínima longitud posible .

Si a es la fracción periódica normada $m-naria$ (*), es decir si $a = m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k})$, se dice entonces que la fracción $m^h(b_1 \ldots b_l, a_1 \ldots a_k)$ *es la descomposición normada del número a en una fracción periódica* $m-naria$.

PROPOSICIÓN *6.1. Sea m un número natural fijo superior a la unidad.*

Para todo número racional positivo dado a existe un entero h y de los números naturales c, n tales que

$(I) \quad a = m^h \frac{c}{n}, \quad (m,n) = 1, \qquad m \nmid c, \qquad (c,n) = 1.$

Además, si el entero h_1 y los número naturales c_1, n_1 cumplen las condiciones

$(I')a = m^{h_1} \frac{c_1}{n_1}, \quad (m, n_1) = 1 \;\; m \nmid c_1, (c_1, n_1) = 1,$

entonces, $h = h_1, c = c_1 \;\; y \;\; n = n_1$.

Demostración. Figúrese el número racional a bajo la forma de una fracción irreducible $a = u/v, (u,v) = 1, u, v \in \boldsymbol{N}$.

Nótese n el máximo común divisor natural del denominador v primo con $m, v = qn$. Entonces, cada divisor primo del número q dividirá m; por lo tanto existen enteros t tales como $\frac{m^t}{q} \in \boldsymbol{N}$. Nótese t_0 el minimo entero t de modo que $\frac{m^{t_0}}{q} u \in \boldsymbol{N}$.Sea $c = \frac{m^{t_0}}{q}.u$, entonces

$a = m^{-t_0}.\frac{c}{n}, \quad m \nmid c, \qquad (c,n) = 1.$

Al plantear $h = -t_0$, se ve que los números h, c, n sastifacen las condiciones (I).

Supóngase que los números h_1, c_1, n_1 cumplen las condiciones (I') ; Entonces $a = m^h.\frac{c}{n} = m^{h_1}.\frac{c_1}{n_1}$. Plantéese $h \geq h_1$, entonces $m^{h-h_1} c n_1 = c_1 n$. Dado que, por hipótesis,$(m,n) = 1 \; y \; m \nmid c_1$, se tiene $m \nmid c_1 n$; por lo tanto $h - h_1 = 0$ y $c n_1 = c_1 n$ y, como resultado, $h = h_1$ y $\frac{c}{n} = \frac{c_1}{n_1}$.

$\frac{c}{n} = \frac{c_1}{n_1}$ siendo irreducibles, $c = c_1$ y $n = n_1$.□

COROLARIO 6.2. *Para un m fijo y un número a racional y positivo dado, existe un único entero h, tal que la fracción a/m^h tenga un denominador primo con m y un numerador no divisible por m.*

DEFINICIÓN. La figuración del número racional positivo a bajo la forma de

$(I) \quad a = m^h.\frac{c}{n},$

donde $(m,n) = 1, , \quad m \nmid c, \quad (c,n) = 1, (c,n) \in \boldsymbol{N}$ se denomirá $m - figuracion$ del número a.El número h sera igualmente denotado $h(a)$.

PROPOSICION 6.3. *Si una fracción periódica $m - naria$*

$m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_K})$ *satisface a la condición $a_K \neq b_l$, entonces su pre-periodo tiene la mínima longitud posible.*

Demostración. De hecho, si $a_k = b_l \quad y \quad l > 1$, entonces $m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k}) = m^{h+1}(b_1 \ldots b_{l-1}, \overline{a_k a_1 \ldots a_{k-1}})$, es decir que se puede disminuir la longitud del pre-periodo de la fracción.□

PROPOSICIÓN 6.4 .*Supóngase que la fracción*

(I) $m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k})$

sea la descomposición en fracción periódica m-naria del número racional positivo a. Sea

(II) $a = m^{h(a)}.\frac{c}{n}$

una m-figuracion del número a. En este caso las afirmaciones siguientes son equivalentes

(α) $b_l \neq a_k$

(β) $A \not\equiv B(mod\ n)$

donde $B = b_1 m^{l-1} + \ldots + b_l$ y $A = a_1 m^{k-1} + \ldots + a_k$,

(γ) $h = h(a)$;

(δ) $\frac{a}{m^h} = \frac{c}{n} = b_1 \ldots b_l, \overline{a_1 \ldots a_k}$.

Demostración. $(\alpha) \rightarrow (\beta)$.Definanse los números $\boldsymbol{A}$ y B en medio de las igualdades siguientes:

(1) $A = a_1 m^{k-1} + \ldots + a_k$, $0 \leq a_1, \ldots, a_k < m$,

(2) $B = a_1 b^{l-1} + \ldots + b_l$, $0 \leq b_1, \ldots, b_l < m$.

Dado que $0 \leq b_l$, $a_k < m$, se deduce de (α) que

(3) $a_k \not\equiv b_l\ (mod\ m)$.

En base de (1), (2) y (3) se concluye que

$$A \not\equiv B(mod\ m);$$

es decir que tiene lugar (β) .

$(\beta) \rightarrow (\gamma)$. Según la hipótesis,

$$a = m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_k}) = m^h\left(b_1 m^{l-1} + \ldots + b_l + \frac{a_1 m^{k-1} + \ldots + a_k}{m^{k-1}}\right),$$

por consiguiente

(4) $a = m^h\left(B + \frac{A}{m^{k-1}}\right) = m^h \frac{B(m^{k-1})+A}{m^{k-1}}$.

Se constata sin duda que

$$B\left(m^k - 1\right) + A \equiv -B + A \equiv -b_l + a_k\ (mod\ m).$$

Según la condición (β) se deduce que

(5) $B\left(m^k - 1\right) + A \not\equiv 0(mod\ m)$,

Es decir que $m + (B\left(m^k - 1\right) + A)$. Por otro lado, debido a (II⟩

Y de (4), se tiene

(6) $a = m^{h(a)}.\frac{c}{n} = m^h \ .\frac{B\left(m^k - 1\right)+A}{m^{k-1}}$.

Conforme a la proposición 6.1 de (5) y de (6) se deduce la igualdad

(7) $h = h(a)$;

$(\gamma) \rightarrow (\delta)$. Por hipótesis,

(8) $a = m^{h(a)}.\frac{c}{n} = m^h(b_1\ , b_l, \overline{a_1 \ldots a_k}\ ,$

De (7) y (8) se tiene

(9) $\frac{a}{m^h}=\frac{c}{n}$ =$b_1 \ldots b_l,\overline{a_1 \ldots a_k}$,

Y por consiguiente, se cumple(δ).

$(\delta) \rightarrow (\alpha)$.De la condición (δ) se deduce que

$\frac{c}{n}=\frac{B\left(m^k-1\right)+A}{m^k-1}$,

Es decir $B(m^k-1)+A=c\,.\frac{m^{k-1}}{n}$. Dado que $(c,m)=1$ y $\left(\frac{m^{k-1}}{n}\,,m\right)=1\,,B\left(m^k-1\right)+A\equiv -B+A\not\equiv 0(mod\ m)$.Por otro lado $-B+A\equiv -b_l+a_k(mod\ m)$. Por lo tanto, $b_l\not\equiv a_k\ (mod\ m)$. Conforme a (1), (2), se deduce que $b_l\neq a_{\Re}$.□

PROPOSICIÓN 6.5. Sea $0\,,\overline{a_1,\ \ldots a_k}$ *la descomposición en fracción periódica* $m-naria$ *del número racional positivo* $r/n\ ,(r\,,n)=1\,,$ *decir*

(1) $r/n=0\ ,\overline{a_1,\ \ldots a_k}\,.$

Entonces la longitud k *del período es divisible por el orden de la clase residual* m mod $n\ ,\vartheta\ (m\ mod\ n\ )\,\big|\,k.$

Demostración. Por hipótesis,

(2) $\frac{r}{n}=\frac{a_1}{m}+\ldots+\frac{a_k}{m_k}+\frac{a_1}{m^{k+1}}+\ldots+\frac{a_k}{m^{2k}}+\ldots$

Plantéese

$A=a_1m^{k-1}+\ldots+a_k\,.$

Entonces, (2) puede escribirse bajo la forma

$\frac{r}{n}=\frac{A}{m^R}+\frac{A}{m^{2R}}+\ldots$

Por lo tanto,

(3) $\frac{r}{n}=\frac{A}{m^R-1}$

Y $r(m^R-1)=nA.$ Ahora bien, como $(n,r)=1$ tenemos $n\,\big|\,\left(\mathrm{m^R}-1\right)$,

Es decir

(4) $m^R\equiv 1\ (\mathrm{mod}\ n)$.

En virtud de la proposición 5.2, se deduce de (4) que k es divisible por el orden de la clase residual m mod n. □

TEOREMA 6.6. *Un número racional* $\frac{r}{n}>0,(r,n)=1,$ *se descompone en fracción puramente periódica m-naria con el periodo más corto*

(1) $0,\ \overline{a_1\ldots a_R},$

si y sólo si se cumple las condiciones

(2) $0\ <\frac{r}{n}\leq 1\,,(\mathrm{m,n})=1.$

En este caso la longitud K *del período más corto es igual al orden de la clase residual* m *mod* n *y la sucesión* $a_1,\ \ldots\,,a_R$ *coincide con la sucesión de cifras en la forma m-ádica del número* $(m^R-1)\cdot r/\,n.$

Demostración. Dado un número racional positivo a representado por una fracción irreducible r/n que satisface las condiciones (2). Plantéese $K = \mathcal{O}$ (m mod n). Si se multiplica el numerador y denominador de la fracción $\frac{r}{n}$ por $\frac{m^R-1}{n}$, se obtiene

(3) $a = \frac{r}{n} = \frac{A}{m^R-1}$.

Sea

(4) $A = a_1 m^{R-1} + \ . \ . \ . + \ a_R$

Una forma m-ádica del número a. En razón de (3)

(5) $a = \frac{r}{n} = \frac{A}{m^R} + \frac{A}{m^{2R}} + . \ . \ .$

De (4) y (5) se deduce que

$$a = \frac{a_1}{m} + \ . \ . \ . + \frac{a_R}{m^R} + \frac{a_1}{m^{R+1}} + . \ . \ . + \frac{a_R}{m^{2R}} + . \ . \ .,$$

dicho de otra manera, se obtuvo una descomposición del número a en una fracción puramente periódica cuyo período es de longitud k:

$$a = 0, \overline{a_1 \ . \ . \ . a_R}.$$

Además, en virtud de la proposición 6.5, la longitud k del período es mínimo y la sucesión $a_1, \ . \ . \ . , a_k$ coincide con el resto de las cifras en la figura m-ádica del número $(m^R - 1) \cdot r/n$.

Supóngase ahora que está en posesión de la descomposición del número $\frac{r}{n}, (r, n) = 1$, en una fracción puramente periódica en tiempo mínimo, $\frac{r}{n} = 0, \ \overline{a_1 \ . \ . \ . a_R}$, Es decir

(1) $\frac{r}{n} = \frac{a_1}{m} + \ . \ . \ . + \frac{a_R}{m^R} + \frac{a_1}{m^{R+1}} + . \ . \ . + \frac{a_R}{m^{2R}} + . \ . \ .$

Sea

(6) $A = a_1 m^{R-1} + \ . \ . \ . + \ a_R$.

Entonces,

(7) $\frac{r}{n} = \frac{A}{m^R} + \frac{A}{m^{2R}} + . \ . \ .$

y, por lo tanto,

(8) $\frac{r}{n} = \frac{A}{m^R-1}$

A causa de (7) y (8), se tiene $0 < A \leq m^R - 1$. Así como de (8), de ello se deduce que

$$0 < \frac{r}{n} \leq 1.$$

De (8) se deduce que $r(m^R - 1) = An$ y como $(n, r) = 1$, se tiene $n \mid (m^R - 1)$, es decir

(9) $m^R \equiv 1 \pmod{n}$

y, por lo tanto, $(m,n)=1$. De (9), según la proposición 5.2, se deduce que $\mathcal{O}(m \bmod n) \mid k$. Por hipótesis, k es el período más corto, así que, en virtud de la proposición 6.5, $k = \mathcal{O}(m \bmod n)$. En razón de (8), $A = (m^R - 1).\frac{r}{n}$. Luego, como en razón de (2),

$$(m^R - 1).\frac{r}{n} = a_1 m^{R-1} + \ldots + a_R.$$

Así, la sucesión $a_1, \ldots, a_k$ de cifras del período de la fracción $0, \overline{a_1 \ldots a_R}$ coincide con la sucesión de cifras de la forma m-ádica del número $(m^R - 1).\frac{r}{n}$.□

TEOREMA 6.7. *Todo número racional positivo a está dotado de una descomposición normada en fracción periódica m-naria $m^h(b_1 \ldots b_l, \overline{a_1 \ldots a_R})$. Además si $a = m^{h(a)}.\frac{c}{n}$ es una m- forma del número a, entonces:*

1) $h = h(a)$;
2) $k = \mathcal{O}(m \bmod n)$;
3) *La sucesión $b_1, \ldots, b_l$ coincide con la sucesión de cifras en la forma m-ádica del número B, donde*

$$B \begin{cases} \left\lfloor \frac{a}{m^h} \right\rfloor & si\ \frac{a}{m^h} \notin Z, \\ \frac{a}{m^h} - 1\ si\ \frac{a}{m^h} \in Z; \end{cases}$$

4) *La sucesión $a_1, \ldots, a_R$ coincide con la sucesión de cifras en la forma m-ádica del número A, donde*

$$A = (m^R - 1)\left(\frac{a}{m^h} - B\right)$$

Demostración. Según la proposición 6.1, existe para el número a un entero h y números naturales c, n tales que

(1) $a = m^h.\frac{c}{n}, \quad (m,n)=1, \quad m+c, \quad (c,n)=1.$

El número c puede ser representado bajo la forma de $c = Bn + r$, donde $0 < r \le n, (r,n) = 1,$ siendo B un número natural, por lo tanto

(2) $\frac{c}{n} = B + \frac{r}{n}, \qquad 0 < \frac{r}{n} \le 1.$

Por lo tanto, se obtiene

$$B = \begin{cases} \left\lfloor \frac{a}{m^h} \right\rfloor & si\ \frac{a}{m^h} \notin Z, \\ \frac{a}{m^h} - 1\ si\ \frac{a}{m^h} \in Z; \end{cases}$$

Según el TEOREMA 6.6, la fracción propia r/n se descompone en una fracción m-naria puramente periódica

(3) $\frac{r}{n} = 0, \overline{a_1 \ . \ . \ . \ a_R}$

Además, la longitud k con el período más corto es igual al orden de la clase residual m mod n,

(4) $k = \mathcal{O}(m \bmod n)$,

y la sucesión $a_1, \ . \ . \ . \ , a_R$ coincide con la sucesión de cifras en la forma m-ádica del número A, donde

$$A = (m^R - 1) \cdot \frac{r}{n} = (m^R - 1)\left(\frac{a}{m^h} - B\right).$$

Sea $B = b_1 m^{l-1} + . \ . \ . + b_l$ una forma m-ádica del número B. Entonces, conforme a (1), (2) y (3), se cumple que,

(5) $\frac{a}{m^h} = \frac{c}{n} = b_1 \ . \ . \ . \ b_l, \overline{a_1 \ . \ . \ . \ a_R}$,

por consiguiente

(6) $a = m^h (b_1 \ . \ . \ . \ b_l, \overline{a_1 \ . \ . \ . \ a_R})$.

Dado que $h = h \ \ (a)$, se deduce de (6), según la proposición 6.4, la desigualdad $b_l \neq a_R$. Sin embargo, conforme a (4) y de la proposición 6.5, la longitud k en el período de la descomposición (6) es mínima. Así, (6) es una descomposición normada del número a en una fracción periódica m-naria.□

Ejercicios

1. Buscar cuantas cifras hay en el período de fracciones decimales, en las que se convierten las fracciones ordinarias, cuyos denominadores son: 3, 7,11, 13, 17, 19, 21.
2. Convertir las siguientes fracciones períodicas decimales en fracciones ordinarias : 0, 35 (62) ; 5, 1 (538); 3, (27); 11, 12 (31).
3. Buscar el denominador de la fracción que se convierte en una fracción puramente períodica que posee tres cifras en el período.
4. Sea p número primo distinto de 2 y 5. Mostrar que si la fracción $1/p$ es convertible en una fracción decimal puramente periódica, con un número par de cifras en el período, entonces las cifras de segunda mitad del período completan hasta nueve las cifras correspondientes a la primera mitad del período. Por ejemplo, $1/7 = 0, \overline{142857}$.
5. Buscar cuantas cifras hay en el período de fracciones decimales en las que son convertidas las fracciones ordinarias cuyos denominadores son: 41, 13.37, 11.13.17, 5.7.19, 2.11.13.
6. ¿Cuál es el valor posible que adopta el denominador de una fracción al convertirse en una fracción decimal puramente periódica con tres cifras en el periodo?
7. ¿Cuál es el valor del denominador de una fracción que se puede convertir en una fracción decimal puramente periódica con cinco cifras en el período?

CAPITULO XIII

ANILLOS

§ 1. Ideales de un anillo. Anillo cociente

Ideal de un anillo: Sea $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un anillo y I un subconjunto del conjunto K. El conjunto I se dice *cerrado en* $\mathcal{K}$ con respecto *a la sustracción* si $a - b \in I$ para todos los elementos a y b de I.

El conjunto I se ldenomina estable *con respecto a la multiplicación a la derecha por los elementos del anillo* $\mathcal{K}$ si $ak \in I$ para todo a de I y todo k de K, es decir cuando en su conjunto I, con cada elemento a de este último, se incluyen todos sus múltiplos a la derecha ak, donde $k \in K$. Se define de forma análoga el conjunto estable con respecto a la multiplicación a izquierda por los elementos del anillo $\mathcal{K}$.

El conjunto I se denomina *estable con respecto a la multiplicación por los elementos del anillo* $\mathcal{K}$ si este es estable con respecto a la multiplicación de la derecha e izquierda por los elementos del anillo $\mathcal{K}$.

DEFINICIÓN: Se denomina *ideal a derecha (izquierda) del anillo* $\mathcal{K}$ a todo sub-conjunto no vacío del conjunto K cerrado en $\mathcal{K}$ con respecto a la sustracción y estable con respecto a la multiplicación a derecha (izquierda) por los elementos del anillo $\mathcal{K}$.

DEFINICIÓN: Se denomina *ideal bilateral del anillo* $\mathcal{K}$ o simplemente *ideal del anillo* $\mathcal{K}$ todo sub-conjunto no vacío del conjunto K si este sub-conjunto es a la vez un ideal a derecha e izquierda del anillo $\mathcal{K}$.

Se deduce de la definición que todo ideal I del anillo $\mathcal{K}$contiene al cero del anillo y cerrado relativo a las tres primeras operaciones principales del anillo.El algebra $\langle I, +, -\rangle$ es un *sub-grupo* del grupo aditivo $\langle K, +, -\rangle$ del anillo. El conjunto $\{\mathcal{O}_{\mathcal{K}}\}$ es un ideal del anillo $\mathcal{K}$ *llamado ideal nulo* o *cero.* El conjunto K es del mismo modo un ideal del anillo $\mathcal{K}$; se integra por múltiples de la unidad del anillo y como resultado, es llamado *ideal unidad (o unitario) del anillo* $\mathcal{K}$. Los ideales cero y unidad se llaman *ideales triviales del anillo* $\mathcal{K}$. Los ideales del anillo distintos de los ideales triviales se llaman *ideales propios del anillo.*

Ejemplos. 1. Sea $\mathcal{Z}$ un anillo de enteros y n un entero fijo. El conjunto $nZ = \{nx \,|\, x \in Z\}$ es un ideal del anillo $\mathcal{Z}$.

2. Sea $\mathcal{K}$ un anillo cualquiera y n un entero fijo. El conjunto $nK = \{nx \,|\, x \in K\}$ es un ideal del anillo $\mathcal{K}$.

3. Sea $\mathcal{K}$un anillo conmutativo y a su elemento fijo. El conjunto $\{\mathcal{K}a \,|\, \mathcal{K} \in K\}$ compuesto por multiples elementos de a es un ideal. Es llamado *ideal principal generado por el elemento* a y denotado (a). En los anillos no conmutativos es necesario distinguir los ideales principales a derecha y los ideales principales a izquierda.

4. Sea $\mathcal{K}$ un anillo conmutativo y $a_1, \ldots, a_n \in K$. El conjunto $\{\mathcal{K}_1 a_1 + \ldots + \mathcal{K}_n a_n \,|\, \mathcal{K}_1, \ldots, \mathcal{K}_n \in K\}$ es un ideal del anillo $\mathcal{K}$. Se llama ideal generado por los elementos $a_1, \ldots, a_n$ y se designa por el simbolo $(a_1, \ldots, a_n)$.

En los anillos no conmutativos es necesario distinguir entre los ideales a derecha de los ideales a izquierda generados por los elementos $a_1, \ldots, a_n$.

Estúdiese las operaciones en los ideales. Se llama *intersección de ideales* I y J del anillo $\mathcal{K}$ el conjunto $I \cap J$. Se define de manera análoga la intersección de toda colección de ideales del anillo.

Se verifica sin dificultad que la intersección de toda colección de ideales del anillo es un ideal de este anillo.

Se denomina *suma de ideales* I y J el conjunto $I + J$ definido por la igualdad

$$I + J = \{x + y \mid x \in I, y \in J\}.$$

Se verifica facilmente que la suma de ideales del anillo es un ideal de este anillo. La adición de los ideales está dotada de las propiedades de la conmutatividad y asociatividad.

Se llama *producto de los ideales* I *y* J del anillo $\mathcal{K}$ el conjunto de todos los elementos de la forma $x_1y_1 + \ldots + x_ny_n$, donde $x_i \in I, y_i \in J$ y n un entero positivo cualquiera. El producto de los ideales I *y* J se escribe $I \cdot J$. Se verifica sin dificultad que el producto de ideales del anillo es un ideal de este anillo.

Notese que el ideal principal (a) generado por el elemento a de un anillo conmutativo $\mathcal{K}$*es una intersección de todos los ideales que contiene el elemento* a y ,como resultado, (a) es el más pequeño de los ideales que contienen a a.

De manera análoga, el ideal $(a_1, \ldots, a_n)$ generado por los elementos $a_1, \ldots, a_n$ del anillo conmutativo $\mathcal{K}$*es una intersección de todos los ideales que contiene los elementos* $a_1, \ldots, a_n$, y como resultado ,$(a_1, \ldots, a_n)$ es el más pequeño de los ideales que contiene $a_1, \ldots, a_n$.

Congruencias y clases residuales según un ideal. Sea I un ideal fijo del anillo $\mathcal{K}$.

DEFINICIÓN. Los elementos a, b del anillo $\mathcal{K}$ son llamados *congruentes que sigun el ideal* I si $a - b \in I$.

La notación $a \equiv b \pmod{I}$ significa que los elementos a y b son congruentes siguidos del ideal I.

PROPOSICIÓN 1.1. *La congruencia que sigue del ideal* I *en el anillo* $\mathcal{K}$ *(en el conjunto* K*) es una relación de equivalencia*.

Demostración. La congruencia que sigue del ideal I es reflexiva, dado que $a - a \in I$ para todo elemento a de k. La congruencia que sigue del ideal I es transitiva, dado que de $a - b \in I$ y $b - c \in I$ se deduce que

$$a - c = (a - b) + (b - c) \in I.$$

La congruencia que sigue del ideal I es simetrica, dado que de $a - b \in I$ se deduce $b - a \in I$. □

DEFINICIÓN: Las clases de equivalencia de la congruencia que siguen el ideal I en el anillo $\mathcal{K}$se denominan *clases residuales que siguen el ideal* I o clases del anillo $\mathcal{K}$ que siguen al ideal I.

La clase residual que contiene el elemento a del anillo $\mathcal{K}$ se denotará $\bar{a}$. Aparentemente, $\bar{a} = a + I$.

TEOREMA 1.2. *Las clases residuales del anillo* $\mathcal{K}$*que siguen al ideal* I *están dotadas de las propiedades siguientes:*

(1) cualesquiera dos clases residuales son iguales, o sean disjuntas.

(2) La reunión de todas las clases residuales del anillo $\mathcal{K}$ *que sigue el ideal* I *coincide con el conjunto* $|\mathcal{K}|$*;*

(3) *Las clases residuales* $\bar{a}$ *y* $\bar{b}$ *que sigue del ideal* I *coinciden si y sólo si* $a \equiv b (mod\ I)$;

(4) Si $c \in \bar{a}$, entonces $\bar{a} = c + I$ (en particular, $\bar{a} = a + I$).

Las propiedades (1)-(4) del TEOREMA expresan las propiedades correspondientes de las clases de grupo $\langle K, +, - \rangle$ según el sub-grupo $\langle I, +, - \rangle$.

Estúdiese las principales propiedades de las congruencias seguidas de un ideal.

PROPIEDAD 1.1. *Las congruencias se pueden sumar y restar miembro a miembro, es decir de*

$a \equiv b$ y $c \equiv d \pmod{I}$

se deduce de

$$a + c \equiv b + d \quad \text{y} \quad a - c \equiv b - d \pmod{I}.$$

Demostración. En efecto, si $a - b \in I$ y $c - d \in I$, entonces

$$a + c - (b + d) \in I \text{ y } (a - c) - (b - d) \in I.$$

Por lo tanto, $a + c \equiv b + d, a - c \equiv b - d (\mathrm{mod}\, I)$. □

PROPIEDAD *1.2. Los dos miembros de la congruencia puede multiplicarse por cualquier entero n, es decir de* $a \equiv b \pmod{I}$ *se deduce que* $na \equiv nb \pmod{I}$, *donde* $n \in Z$.

Demostración. De $a - b \in I$ se deduce que $na - nb = n(a - b) \in I$.□

PROPIEDAD 1.3. Los dos miembros de la congruencia pueden multiplicarse a derecha y a izquierda por cualquier elemento del anillo, es decir de

$$a \equiv b \pmod{I} \text{ y } c \in |\mathcal{K}|$$

se deducen las congruencias

$$ca \equiv cb \pmod{I}, \quad ac \equiv bc \pmod{I}.$$

Demostración. El conjunto de los elementos del ideal I es estable en relación a la multiplicación por los elementos del anillo. Por tanto, para todo elemento c del anillo $\mathcal{K}$ de $a - b \in I$ se deduce $ca - cb \in I$ y $ac - bc \in I$.□

PROPIEDAD 1.4. *Las congruencias pueden multiplicarse miembro a miembro, es decir si*

$$a \equiv b, \quad c \equiv d \pmod{I}, \text{ entonces } ac \equiv bd \pmod{I}.$$

Demostración. De hecho, si $a - b \in I$ y $c - d \in I$, entonces, en virtud de la estabilidad del ideal I en relación a la adición y a la multiplicación por los elementos del anillo, resulta

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) \in I.$$□

Anillo cociente. Sea I un ideal del anillo $\mathcal{K} = \langle K, +, -, 1\rangle$. Se estableció anteriormente que la congruencia de módulo I es una relación de equivalencia en el conjunto K. *Las clases de equivalencia llamadas clases residuales o clases del anillo* $\mathcal{K}$ *que sigue el ideal* I *o módulo* I. *El conjunto de todas las clases residuales se denomina conjunto cociente* K *módulo* I *y denotado* K/I.

Las propiedades 1.1-1.4 de las congruencias que siguen el ideal muestran que las congruencias módulo I es una congruencia en el anillo $\mathcal{K}$ (una congruencia relativamente a todas las operaciones principales del anillo $\mathcal{K}$). Por lo tanto, según el TEOREMA 3.1.9, encontramos en condiciones de definir las operaciones $+, -, \cdot, \overline{1}$ asociadas a las operaciones principales del anillo $\mathcal{K}$ en el conjunto cociente K/I de la siguiente manera:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad -\bar{a} = \overline{(-a)}, \quad \overline{ab} = \overline{ab}, \quad \overline{1} = 1 + I$$

para todos los elementos $\bar{a}$, $\bar{b}$ de K/I.

Esta definición de las operaciones sobre el conjunto cociente K/I es correcta, puesto que no depende de la elección de los elementos a, b en las clases $\bar{a}$ y $\bar{b}$ respectivamente.

DEFINICIÓN. El algebra $\langle K/I\ , +, -,\ \cdot\ , \bar{1}\rangle$ es nombrada *anillo cociente del anillo $\mathcal{K}$ módulo I* y denotada $\mathcal{K}/I$.

TEOREMA 1.3. Sea I el ideal del anillo $\mathcal{K}$. En este caso el algebra $\mathcal{K}/I = \langle K/I\ , +, -,\ \cdot\ , \bar{1}\rangle$ es un anillo.

Demostración. El algebra $\langle K/I\ , +, -\rangle$ es un grupo abeliano dado que es un grupo cociente del grupo aditivo $\langle K, +, -\rangle$ del anillo $\mathcal{K}$ que sigue del sub-grupo $\langle I, +, -\rangle$ (ver TEOREMA 10.4.2).

Le algebra $\langle \mathrm{K/I}\ ,\ \cdot, \bar{1}\rangle$ es un monoide. En efecto, en virtud de la asociatividad de la multiplicación en $\mathcal{K}$ para todos $\bar{a},\ \bar{b},\ \bar{c}$ de K/I, se tiene

$$\bar{a}.\left(\bar{b}\,.\,\bar{c}\right) = \bar{a}\,.\left(\overline{bc}\right) = \overline{a\,(bc)} = \overline{(ab)c} = \left(\bar{a}\bar{b}\right).\bar{c} = \left(\bar{a}\,.\,\bar{b}\right).\bar{c},$$

dicho de otra manera, la multiplicación en el algebra $\mathcal{K}$/I es asociativa
Además,

$$\bar{a}.\ \bar{1} = \overline{a\,.1} = \bar{a} = \ \bar{1}\,.\bar{a}\ \text{ Para todo } \bar{a} \text{ de K/I,}$$

Es decir $\bar{1}$ es un elemento neutro con respecto a la multiplicación en el algebra $\mathcal{K}$/I.

En $\mathcal{K}$/I la multiplicación es distributiva respecto a la adición. En efecto, en virtud de la distributividad de la multiplicación respecto a la adición en el anillo $\mathcal{K}$ para todos $\bar{a},\ \bar{b},\ \bar{c}$ de K/I se cumple

$$\left(\bar{a} + \bar{b}\right).\ \bar{c} = \overline{a+b}\,.\,\bar{c} = \overline{a+b.c} = \overline{ac+bc} =$$
$$= \bar{a}\bar{c} + \overline{bc} = \bar{a}\ \cdot\bar{c} + \ \bar{b}\ \cdot\bar{c}$$

De manera análoga, se demuestra que $\bar{c}\left(\bar{a} + \bar{b}\right) = \bar{c}\ \cdot\bar{a} + \bar{c}\ \cdot\bar{b}$. □

TEOREMA de epimorfismos de anillos. Sean $\mathcal{K}$ y $\mathcal{K}'$ anillos:

$$\mathcal{K} = \langle K, +, -,\ \cdot\ , 1\rangle, \quad \mathcal{K}' = \langle \mathrm{K}', +, -,\ \cdot\ , 1'\rangle.$$

TEOREMA 1.4. *Un núcleo de homomorfismo del anillo $\mathcal{K}$ en el anillo $\mathcal{K}'$ es un ideal del anillo $\mathcal{K}$.*

Demostración. Sea $Ker\ f$ un núcleo de homomorfismo f del anillo $\mathcal{K}$ en el anillo $\mathcal{K}'$, es decir $Ker\ \ f = \left\{x \in \mathcal{K}\ \middle|\ f(x) = 0'\right\}$, donde $0'$ es el cero del anillo $\mathcal{K}'$. El conjunto $Ker\ \ f$ no es vacío, ya que $0\ \in Ker\ f$. Para todos a, b de $Ker\ f$, se obtiene

$$f\ (a-b) = f\ (a) - \ f\ (b) = 0' - 0' = 0'\ ,$$

es decir, el conjunto $Ker\ f$ es cerrado en $\mathcal{K}$ respecto a la sustracción.

Para todo a de $Ker\ f$ y todo k de K , se obtiene

$$f(ka) = f(k)\cdot f(a) = f(k)\cdot 0' = 0',$$

es decir $ka \in\ Ker\ f$. De manera análoga se demuestra que $ak \in\ Ker\ f$.

Así, $Ker\ f$ es estable respecto a la multiplicación por los elementos de K. Por consiguiente, el núcleo de homomorfismo f es un ideal del anillo $\mathcal{K}$. □

PROPOSICIÓN 1.5. *Sea f un homomorfismo del anillo $\mathcal{K}$en el anillo $\mathcal{K}'$ de núcleo I. Para todos $a\ , b$ de K la igualdad $f\ (a) = f\ (b)$ se verifica si y sólo si $\bar{a} = \ \bar{b}$.*

Demostración. Sea $f\ (a) = f\ (b)$. Entonces,

(1) $f\ (a-b) = f\ (a) - f\ (b) = 0'$,

puesto que f es un homomorfismo. Por tanto $a - b \in I$ y como resultado, $\bar{a} = \overline{b}$.

Véase ahora que $\bar{a} = \overline{b}$. Entonces, $a - b \in I$ y $f\ (a-b) = 0'$, dado que $I = K\text{er}\, f$. De allí tomando en cuenta (1), se obtiene

$$f\ (a-b) = f\ (a) - f\ (b) = 0' \quad \text{Y} \quad f\ (a) = f\ (b). \square$$

TEOREMA 1.6. *Sea f un epimorfismo del anillo $\mathcal{K}$ en el anillo $\mathcal{K}'$ del núcleo I. Entonces el anillo cociente $\mathcal{K}/I$ es isomorfo al anillo $\mathcal{K}'$.*

Demostración. Por hipótesis, $I = K\text{er}\, f$. Sea $\overline{K} = K/I$ el conjunto de todas las clases residuales del anillo $\mathcal{K}$ módulo I y

$$\mathcal{K}/I = \langle K/I\ , +\ , -,\ \cdot\ , \overline{1}\rangle,$$

donde $\overline{1} = 1 + I$. Se designa por h la función K/I en $|\mathcal{K}'|$, que se define de la manera siguiente:

(1) $h(\bar{a}) = f\ (\bar{a})$ para cada elemento $\bar{a}$ de K.

En virtud de la proposición 1.5, el valor de $h\ (\bar{a})$ es independiente de la selección del representante a en la clase $\bar{a}$. Luego, la función h respeta las operaciones principales del anillo $\mathcal{K}/I$. En efecto, $h\ (\overline{1}) = 1_{\mathcal{K}'}$ y para todos $\overline{\text{a}}$, $\overline{\text{b}}$, de K, se obtiene:

$$h\big(\bar{a} + \bar{b}\big) = h\big(\overline{a+b}\big) = f(a+b) = f(a) + f(b) = h(\bar{a}) + h\big(\bar{b}\big)\ ;$$
$$h(-\bar{a}) = h\ \big((\overline{-a})\big) = f(-a) = -f(a) = -h\ (\bar{a});$$
$$h\ \big(\bar{a}\cdot\bar{b}\big) = h\ \big(\overline{ab}\big) = f(ab) = f(a)\cdot f(b) = h(\bar{a})\cdot h\ \big(\bar{b}\big).$$

Por hipótesis, f es una función de $|\mathcal{K}|$ sobre $|\mathcal{K}'|$. En virtud de (1), se deduce que h es una función del conjunto K sobre el conjunto $|\mathcal{K}'|$. La función h es inyectiva. De hecho, en virtud de (1), de la igualdad $h\ (\bar{a}) = h\big(\bar{b}\big)$ se deduce $f\ (a) = f\ (b)$; en virtud de la proposición 1.5, se deduce que $\bar{a} = \overline{b}$. Por consiguiente, h es un isomorfismo del anillo cociente $\mathcal{K}/I$ sobre el anillo $\mathcal{K}'$. $\square$

Característica de un anillo. Sea $\mathcal{K} = \langle K, +, -,\ \cdot, e\rangle$ un anillo con unidad e. En el grupo aditivo $\langle K, +, -\rangle$ del anillo, el elemento e está dotado sea de orden finito $\mathcal{O}(e) = m$, sea de orden infinito $\mathcal{O}(e) = \infty$.

DEFINICIÓN. Se dice que el anillo $\mathcal{K}$ posee una característica finita m si en el grupo aditivo del anillo, la unidad del anillo tiene un orden finito m. Se dice que el anillo $\mathcal{K}$ tiene una característica nula si la unidad del anillo $\mathcal{K}$ esta dado de un orden infinito.

Puesto que todo cuerpo $\mathcal{F}$ es un anillo, se puede hablar de la característica de un cuerpo $\mathcal{F}$. Establézcase denotar $ch(\mathcal{K})$ la característica del anillo $\mathcal{K}$.

Ejemplos. 1. Sea $\mathcal{Z}$ un anillo de enteros. Para todo entero positivo n, se tiene la condición $n\cdot 1 \neq 0$, es decir $\mathcal{O}(1) = \infty$. Por consiguiente, un anillo de enteros tiene una característica nula.

2. Sea m un número natural cualquiera diferente de cero. El anillo cociente $\mathcal{Z}_m = \mathcal{Z}/(m)$ admite una característica finita m, dado que $\overline{1}$, unidad del anillo $\mathcal{Z}_m$, posee el orden m.

3. Sea $\mathcal{K}$ cualquier anillo numérico. Entonces, para todo entero positivo n satisface la desigualdad $n \cdot 1 \neq 0$ y, por consiguiente, $\mathcal{O}(1) = \infty$. Así que, todo anillo numérico es de característica nula.

4. Sea $\mathcal{F}$ un cuerpo de característica $m, \mathcal{K}$ un anillo de las matrices cuadradas sobre $\mathcal{F}$ y E una matriz unidad (unidad del anillo).

El anillo $\mathcal{K}$ tiene la característica m, ya que $\mathcal{O}(E) = \mathcal{O}(1_{\mathcal{F}}) = m$.

TEOREMA 1.7. *La característica de un dominio de integridad es bien cero, o bien un número primo.*

Demostración. Sea $\mathcal{K}$ un dominio de integridad y e la unidad del anillo $\mathcal{K}$. Si $\mathcal{O}(e) = \infty$, entonces $\mathcal{K}$ es de característica nula.

Si $\mathcal{O}(e) = 1$, entonces $e = 1_{\mathcal{K}} = 0_{\mathcal{K}}$. Sin embargo $1_{\mathcal{K}} \neq 0_{\mathcal{K}}$, dado que $\mathcal{K}$ es un dominio de integridad. Por tanto $\mathcal{O}(e) \neq 1$.

Ahora admítase que $\mathcal{O}(e) = m$ es un número compuesto natural positivo: $m = st$, $1 < s$, $t < m$. por lo tanto,

$$0 = m \cdot e = (st) \cdot e = (se) \cdot (t \cdot e).$$

Como $\mathcal{O}(e) = m$ y $1 < s$, $t < m$, Tenemos $s \cdot e \neq 0$ y $t \cdot e \neq 0$, pero puesto que $\mathcal{K}$ es un dominio de integridad, se deduce que $(s \cdot e) \cdot (t \cdot e) = m \cdot e \neq 0$. Se ha llegado a una contradicción con el supuesto que m es un número compuesto. Por tanto, m es un número primo.□

TEOREMA 1.8. Sea p un elemento primo del anillo $\mathcal{Z}$. Entonces el anillo cociente $\mathcal{Z}_p = \mathcal{Z}/(p)$ es un cuerpo.

Demostración. Sea $\bar{a}$ todo elemento no nulo del anillo $\mathcal{Z}_p$. Se trata de mostrar que $\bar{a}$ es inversible en el anillo $\mathcal{Z}_p$.

La condición $\bar{a} \neq \bar{0}$ refleja el hecho de que p no divide a. Por tanto, p y a son primos entre ellos. Por lo tanto existen enteros m y n tales que $mp + na = 1$. Por consiguiente, $\bar{n} \cdot \bar{a} = \bar{1}$ es decir que el elemento $\bar{a}$ es inversible en el anillo $\mathcal{Z}_p$. Así, el anillo $\mathcal{Z}_p$ es un cuerpo. □

El mínimo sub-anillo de un anillo. El sub-anillo generado por la unidad del anillo $\mathcal{K}$ contiene en todo sub anillo de este anillo.

DEFINICIÓN. Un sub-anillo del anillo $\mathcal{K}$ generado por su unidad se denomina *el más pequeño* o *el sub anillo principal del anillo* $\mathcal{K}$.

Sea e la unidad del anillo $\mathcal{K} = \langle K, +, -, \cdot, e\rangle$ $E = \{ne \mid n \in Z\}$ y $\mathcal{E}$ el más pequeño sub-anillo del anillo $\mathcal{K}$. E es entonces el conjunto de base del anillo $\mathcal{E}$: $\mathcal{E} = \langle E, +, -, \cdot, e\rangle$. Se verifica sin dificultad que el anillo $\mathcal{E}$ es una intersección de todos los sub-anillos del anillo $\mathcal{K}$.

TEOREMA 1.9. *Sea m la característica del anillo $\mathcal{K}$ y $\mathcal{E}$ el más pequeño sub-anillo de este anillo. Si $m = 0$, entonces $\mathcal{E}$ es isomorfo en el anillo $\mathcal{Z}$ de los enteros. Si por el contrario, $m > 0$, entonces $\mathcal{E}$ es isomorfo en el anillo cociente $\mathcal{Z}/(m)$.*

Demostración. Considérese la función h del conjunto $\mathcal{Z}$ en E tal que

(1) $h(n) = ne$ para todo entero n.

En virtud de (1), h es una función del conjunto $\mathcal{Z}$ sobre E y, además, h respeta las operaciones principales del anillo $\mathcal{Z}$, es decir

$h(n+s) = h\,(n) + h\,(s), \qquad h\,(-n) = -h(\,n),$
$h\,(n \cdot s) = h\,(n) \cdot h\,(s), \qquad h\,(1) = e$

Para todo entero n y s. Por tanto, h es un epimorfismo del anillo $\mathcal{Z}$ sobre el anillo $\mathcal{E}$.

Muéstrese que $K\text{er}\ h = (m)$. En efecto, puesto que $h\,(m) = me = 0$, se tiene $(m) \subset K\text{er}\ h$. Luego, si $s \in K\text{er}\ h$, entonces $h(s) = 0$ y, como resultado, $s \cdot e = 0$. Por otra parte, puesto que $\mathcal{O}(e) = m$, se tiene $s \in (m)$, en virtud del TEOREMA 10.3.1. De este modo, $K\text{er}\ h \subset (m)$; por consiguiente, $K\text{er}\ h = (m)$.

Según el TEOREMA de epimorfismo de un anillo, $\mathcal{Z}/K\text{er}\ h \cong \mathcal{E}$.

Pero dado que $K\text{er}\ h = (m)$, $\mathcal{E} \cong \mathcal{Z}/\,(m)$. En particular, $\mathcal{E} \cong \mathcal{Z}/\,(0)$ para $m = 0$. Por consiguiente, para $m = 0$ el anillo $\mathcal{E}$ es isomorfo en el anillo $\mathcal{Z}$ de los enteros. □

COROLARIO 1.10. *Sea $\mathcal{K}$ un dominio de integridad de característica $m > 0$. Entonces $\mathcal{E}$, el más pequeño sub-anillo del anillo $\mathcal{K}$, es un cuerpo.*

Demostración. Puesto que $m > 0$, entonces según el TEOREMA 1.7, m es primo. Por consiguiente, según el TEOREMA 12.3.7, $\mathcal{Z}/\,(m)$ es un cuerpo. En virtud del TEOREMA 1.9, el anillo $\mathcal{E}$ es isomorfo al cuerpo $\mathcal{Z}/\,(m)$ y, por consiguiente, es en sí mismo un cuerpo. □

Ejercicios

1. Sea n un entero cualquiera y $nZ = \{nx\,, x \in Z\}$. Mostrar que para todo n el conjunto nZ es un ideal del anillo $\mathcal{Z}$. Mostrar que todo ideal del anillo $\mathcal{Z}$ es un conjunto nZ para un cierto número natural n.
2. Mostrar que las operaciones binarias de intersección y de algunos ideales son conmutativas y asociativas.
3. Demostrar que la intersección de ideales a izquierda(a derecha) del anillo es un ideal a izquierda(a derecha) del anillo.
4. Mostrar que un cuerpo no tiene más ideales que ideal nulo y el ideal unidad.
5. Sea $\mathcal{V}$ un espacio vectorial de dimensión finita sobre el cuerpo $\mathcal{F}$. Sea $\mathcal{K}$ un anillo de operadores lineales del espacio $\mathcal{V}$. Demostrar que el anillo $\mathcal{K}$ está necesitado de ideales bilaterales diferentes de los ideales nulos y unidad.
6. Buscar todos los ideales del anillo $\mathcal{Z}_{12}$.
7. Demostrar que un dominio de integridad finita es un cuerpo.
8. Sea $\mathcal{K}$ un anillo y n un entero. Mostrar que el conjunto $\{x \in K | nx = 0_{\mathcal{K}}\}$ es un ideal del anillo $\mathcal{K}$.
9. Sea $\mathcal{F}$ un cuerpo finito compuesto de m elementos. Demostrar que $a^m = a$ para todo elemento a del cuerpo $\mathcal{F}$.
10. Buscar todos los automorfismos de un cuerpo de números complejos cuyos números reales se mantienen invariantes.
11. Demostrar que para todo isomorfismo de los cuerpos numéricos, los sub cuerpos de números racionales constituye una función idéntica.
12. Demostrar que el anillo de las matrices de la forma.

$$\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}$$

Con a, b, c, d reales es isomorfo al cuerpo (del anillo con división) de los cuaterniones $a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ sobre los cuerpos de números reales.

13. Demostrar que el más pequeño sub cuerpo, de todo cuerpo de característica nula es isomorfo al cuerpo de los números racionales.

14. Demostrar que $\mathcal{Z}_6/2Z_{6\cong}.\mathcal{Z}_2$ y $\mathcal{Z}_6/3Z_6 \cong \mathcal{Z}_3$.

15. Sea n un divisor positivo del número natural m. Demostrar que $\mathcal{Z}_m/nZ_m \cong \mathcal{Z}_n$.

16. Demostrar que el dominio de la integridad que contengan sólo tres elementos, es isomorfo al anillo cociente$\mathcal{Z}/3Z$.

17. Demostrar que los cuerpos $\mathcal{Q}(\sqrt{7})$ y $\mathcal{Q}(\sqrt{11})$ no son isomorfos.

§ 2. Cuerpos de cocientes de un dominio de integridad

Cuerpos de cocientes de un dominio de integridad. El problema de posibilidad de inmersión de un dominio de integridad en un cuerpo es de mayor importancia.

DEFINICIÓN. Un cuerpo $\mathcal{F}$ se llama *cuerpo de cocientes de un domino de integridad* $\mathcal{K}$ si se cumplen las condiciones:

(α) $\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{F}$;
(β) para cualquier x de F existe en $\mathcal{K}$ los elementos a y b tales que $x = a \cdot b^{-1}$.

TEOREMA 2.1. *Para cualquier domino de integridad existe un cuerpo de cocientes.*
Demostración. Sea $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un dominio de integridad, $K^* = K \setminus \{0\}$ y

$K \times K^*\{\langle a, b\rangle | a \in K, b \in K^*\}$.

defínase sobre el conjunto $K \times K^*$ la relación binaria $\equiv$ de la manera siguiente:

$\langle a, b\rangle \equiv \langle c, d\rangle$ si y sólo si a$d = bc$.

Denomínese *congruencia sobre* $K \times K^*$ a esta relación. La congruencia es reflexiva, simétrica y transitiva.

La reflexividad y simetría son evidentes. La transitividad se manifiesta igual. En efecto, de las premisas se deduce que $ad = bc,\ cf = de, d \neq 0$. Al multiplicar los dos elementos de la primera igualdad por f, y la segunda por b, se obtienen: $adf = bcf = bed$ y por consiguiente, $adf = bed$. Esta última igualdad implica $af = be$, dado que $\mathcal{K}$ es un dominio de integridad y $d \neq 0$. Por lo tanto, $\langle a, b\rangle \equiv \langle e, f\rangle$.

Así, la congruencia es una relación de equivalencia sobre el conjunto $k \times K^*$. La clase de equivalencia que contiene la pareja $\langle a, b\rangle$ se denota $[a, b]$, el conjunto cociente $K \times K^* /\equiv$ por F_1. Obsérvese que para cualquier $[a, b]$ y $[c, d]$ de F_1, se tiene

(1) $[a, b] = [c, d]$ si y sólo si $ad = bc$.

Defínase sobre el conjunto $K \times K^*$ las operaciones $\oplus, \ominus, \odot$:

$\langle a, b\rangle \oplus \langle c, d\rangle = \langle ad + bc, bd\rangle$;
$\ominus \langle a, b\rangle = \langle -a, b\rangle$;
$\langle a, b\rangle \odot \langle c, d\rangle = \langle ac, bd\rangle$.

$\mathcal{K}$ siendo un dominio de integridad, $b \neq 0$ y $d \neq 0$ implica que $bd \neq 0$. Por tanto, el conjunto $K \times K^*$ está cerrado relativamente a las operaciones $\oplus, \ominus$, y $\odot$. Se ve fácilmente que las operaciones de adición y multiplicación son conmutativas.

Demuéstrese que la congruencia sobre $K \times K^*$ es una congruencia para las operaciones $\oplus, \ominus$, y $\odot$. Dado que las operaciones de adición y multiplicación son conmutativas, es suficiente demostrar que de la condición

(2) $\langle a, b\rangle \equiv \langle a', b'\rangle$

resultan las relaciones:

(3) $\langle a, b\rangle \oplus \langle c, d\rangle \equiv \langle a', b'\rangle \oplus \langle c, d\rangle$;
(4) $\ominus \langle a, b\rangle \equiv \ominus \langle a'b'\rangle$;
(5) $\langle a, b\rangle \odot \langle c, d\rangle \equiv \langle a', b'\rangle \odot \langle c, d\rangle$.

La verificación de (3) lleva al establecimiento de la relación

$$\langle ad + bc, bd\rangle \equiv \langle a'd + b'c, b'd\rangle.$$

Esta relación se reduce a la igualdad

$$(ad + bc)b'd = (a'd + b'c)bd$$

que, a su vez, puede reemplazarse por la igualdad $ab'd^2 = a'bd^2$, que se obtiene a partir de la igualdad $ab' = a'b$. Esta última igualdad se deduce de la condición (2).

La verificación de (4) lleva al establecimiento de la relación

$$\langle -a, b\rangle \equiv \langle -a'b'\rangle,$$

reduce a la igualdad $(-a)b' = (-a')b$ que, a su vez, es remplazada por la igualdad $ab' = a'b$ válido con forme a la condición (2).

La verificación de (5) lleva al establecimiento de la relación

$$\langle ac, bd\rangle \equiv \langle a'c, b'd\rangle,$$

se reducen a la igualdad $ac.b'd = a'c.bd$ que, a su vez, se obtiene a partir de la igualdad $ab' = a'b$, verdadera conforme a la condición (2).

En resumen, se estableció que la congruencia sobre el conjunto $K \times K^*$ es una congruencia para las operaciones $\oplus, \ominus, \odot$. Según el TEOREMA 3.1.9 sobre las congruencias, las *operaciones* $+, -,$. se definen sobre el conjunto cociente F_1 mediante las fórmulas siguientes:

(6) $[a, b] + [c, d] = [ad + bc, bd]$;
(7) $-[a, b] = [-a, b]$;
(8) $[a, b] \cdot [c, d] = [ac, bd]$,

Además, los valores de las operaciones de esta manera definida son independientes de la elección arbitraria de las parejas $\langle a, b\rangle$ y $\langle c, d\rangle$ en las clases de equivalencia $[a, b]$ y $[c, d]$ respectivamente.

Para cualquier elemento a de K supóngase $\overline{a} = [a, 1]$, en particular, $\overline{0} = [0,1], \overline{1} = [1,1]$. sobre la base de (1) se concluye que:

$[a, b] = \overline{0}$ si y sólo si $a = 0$;
$[a, b] = \overline{1}$ si y sólo si $a = b$;
$[a, b] = [ac, bc]$ para cualquier $c \neq 0$.

Demuéstrese que el álgebra $f_1 = \langle F_1, +, -, \cdot, \overline{1}\rangle$ es un cuerpo. Una verificación directa demuestra que la adición en F_1, resulta

$$[a, b] + (-[a, b]) = \overline{0}.$$

Por tanto, el álgebra $\langle F_1, +, -\rangle$ es un *grupo abeliano.*

Una verificación directa demuestra igualmente que la multiplicación en f_1 comutativa y asociativa y $\overline{1}$ es un elemento neutro respecto a la multiplicación. Por lo tanto, el algebra $\langle F_1, \cdot, \overline{1}\rangle$ es un *monoide conmutativo.*

Muéstrese que la multiplicación en f_1 es distributiva respecto a la adición, es decir que para cualquier $[a, b], [c, d], [e, f]$ de F_1, se tiene

$$([a, b] + [c, d])[e, f] = [a, b][e, f] + [c, d][e, f].$$

Es necesario demostrar que

$$[ade + bce, bdf] = [ae \cdot df + ce \cdot bf, bf \cdot df],$$

O

$$\langle ade + bce, bdf\rangle \equiv \langle (ade + bce)f, bdf \cdot f\rangle (f \neq 0).$$

La última relación es la consecuencia de $\langle a_1, b_1\rangle \equiv \langle a_1 f, b_1 f\rangle$ para cualquier $a_1 f, b_1 f$ con $f \neq 0$.

Así, el álgebra $\mathcal{F}_1$ es un *anillo conmutativo*. En el anillo $\mathcal{F}_1$ satisface la condición $\overline{0} \neq \overline{1}$, puesto que $0 \cdot 1 \neq 1 \cdot 1$ en el cuerpo $\mathcal{F}$.

En el anillo $\mathcal{F}_1$ cualquier otro elemento de $\overline{0}$ es inversible. En efecto, si $[a, b] \neq \overline{0}$, entonces $a \neq 0, [b, a] \in F_1$ y $[a, b] \cdot [b, a] = \overline{1}$. En resumen, se estableció que el álgebra $\mathcal{F}_1$ es un cuerpo.

El cuerpo $\mathcal{F}_1$ contiene un sub-anillo isomorfo en el anillo $\mathcal{K}$. De hecho, considérese el conjunto $\mathcal{K}_1 = \{a, 1 | a \in K\}$. este conjunto está cerrado en $\mathcal{F}_1$, de manera que

$$(9)\ [a, 1] + [b, 1] = [a + b, 1], -[a, 1] = [-a, 1], [a, 1][b, 1] = [ab, 1], [1,1] \in K_1$$

Para cualquier $[a,1],[b,1]$ de K_1. Por tanto, el álgebra $\mathcal{K}_1 = \langle K_1, +, -, \cdot, \overline{1}\rangle$ es un sub-anillo del cuerpo $\mathcal{F}_1$. Defínase la *aplicación* h_1 *del conjunto* K_1 *en* K de la manera siguiente:

$$h_1([a,1]) = a \text{ para cada } a \text{ de } K.$$

h_1 es aparentemente una aplicación inyectiva del conjunto K_1 sobre K. Conforme a (9), la aplicación h_1 respeta las operaciones principales del anillo K_1, es decir

$$h_1(\overline{a}+\overline{b}) = a+b, \quad h_1(-\overline{a}) = -a, \quad h_1(\overline{a}\overline{b}) = ab, \quad h_1(\overline{1}) = 1.$$

Así, h_1 es un *isomorfismo del anillo* $\mathcal{K}_1$ sobre el anillo $\mathcal{K}$. Por tanto, el cuerpo $\mathcal{F}_1$ contiene el sub-anillo $\mathcal{K}_1$ isomorfismo en el anillo de partida $\mathcal{K}$.

Ahora es necesario construir para el cuerpo $\mathcal{F}_1$ un nuevo cuerpo isomorfo al cuerpo $\mathcal{F}_1$ y que contenga el sub-anillo $\mathcal{K}$. Con este fin, se remplaza en el conjunto F_1 cada elemento $[a,1]$ por el elemento a (imagen del elemento $[a,1]$ después de efectuar la operación h_1), dejando todos los otros elementos del conjunto F_1 iguales. Supóngase $F = (F_1 \setminus K_1) \cup K$. Nótese h la aplicación siguiente del conjunto F_1 sobre F:

$$h(x) = \begin{cases} h_1(x) \; si \; x \in K_1, \\ x \qquad si \; x \in F_1 \setminus K_1. \end{cases}$$

La aplicación h es una *aplicación inyectiva del conjunto* F_1 sobre F que prolonga la aplicación h_1.

Defínase sobre el conjunto F las operaciones $+, -, \cdot$ por las fórmulas

$$(*) \qquad \begin{aligned} &\alpha+\beta = h\big(h^{-1}(\alpha)+h^{-1}(\beta)\big), \\ &-\alpha = h\big(-h^{1}(\alpha)\big), \\ &\alpha\cdot\beta = h\big(h^{-1}(\alpha)\cdot h^{-1}(\beta)\big) \quad (\alpha,\beta \in F). \end{aligned}$$

Nótese que $1 = h(\overline{1})$. Considérese el álgebra $\mathcal{F} = \langle F, +, -, \cdot, 1\rangle$. Sobre la base de fórmulas $(*)$ se concluye que las fórmulas siguientes son verdaderas:

$$\begin{aligned} &h^{-1}(\alpha+\beta) = h^{-1}(\alpha)+h^{-1}(\beta), \\ &h^{-1}(-\alpha) = -h^{-1}(\alpha) \quad (\alpha,\beta \in F), \\ &h^{-1}(\alpha\beta) = h^{-1}(\alpha)\cdot h^{-1}(\beta), \\ &h^{-1}(1) = \overline{1}. \end{aligned}$$

Esas fórmulas demuestran que h^{-1} es un *isomorfismo del álgebra* $\mathcal{F}$ sobre el cuerpo $\mathcal{F}_1$. Por tanto, el álgebra $\mathcal{F}$ es un cuerpo. En este caso $\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{F}$ puesto que $K \subset F$ y, conforme a las fórmulas $(*)$, las operaciones $+, -, \cdot$ en $\mathcal{F}$ prolongan las principales operaciones correspondientes al anillo $\mathcal{K}$. En efecto, para cualquier α, β de K, resulta:

$$\alpha+\beta = h([\alpha,1]+[\beta,1]) = h([\alpha+\beta,1]) = \alpha+\beta;$$

$$\begin{aligned} &-\alpha = h(-[\alpha,1]) = h([-\alpha,1]) = -\alpha; \\ &\alpha\cdot\beta = h([\alpha,1]\cdot[\beta,1]) = h([\alpha\beta,1]) = \alpha\beta. \end{aligned}$$

Cada elemento x de F puede ser representado bajo forma de cociente de elementos del anillo $\mathcal{K}$. En efecto, si $h^{-1}(x) = [a, b]$, donde $a, b \in K$ y $b \neq 0$, entonces

$$[a, b] = [a, 1] \cdot [1, b] \text{ y } h^{-1}(x) = \overline{a} \cdot \left(\overline{b}\right)^{-1}.$$

Por lo tanto,

$$x = h\left(\overline{a} \cdot \overline{b}^{-1}\right) = h(\overline{a}) \cdot h\left(\overline{b}^{-1}\right) = a \cdot b^{1},$$ y , por consiguiente, $x = a \cdot b^{-1}$.

En resumen, se estableció que $\mathcal{F}$ es un cuerpo que satisface a las condiciones: $(\alpha)\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{F}$; (β) para cualquier x de F existe en $\mathcal{K}$ los elementos a, b tales como $x = a \cdot b^{-1}$. Por tanto, $\mathcal{F}$ es un cuerpo de cocientes por el domino integro $\mathcal{K}$. □

Isomorfismo de cuerpos de cocientes. Muéstrese que cualquier dominio de integridad contiene un cuerpo único de cocientes en el isomorfismo cercano.

TEOREMA 2.2. Sea $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un domino de integridad. Sean $\mathcal{F} = \langle F, +, -, \cdot, 1\rangle$ y $\mathcal{P} = \langle P, \oplus, \ominus, \odot, 1\rangle$ los cuerpos cocientes del anillo $\mathcal{K}$. Existe entonces un isomorfismo del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$ que hace pasar cada elemento del anillo $\mathcal{K}$ en el mismo.

Demostración. Por hipótesis, $\mathcal{F}$ es un cuerpo de cocientes, por tanto cumple las condiciones:

(α) $\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{F}$;

(β) para cualquiera x de F existe en K los elementos a, b tales como $x = a \cdot b^{-1}$. A continuación, por hipótesis, $\mathcal{P}$ es otro cuerpo de los cocientes del anillo $\mathcal{K}$, por lo tanto, se cumplen las condiciones:

(γ) $\mathcal{K}$ es un sub-anillo del cuerpo $\mathcal{P}$;

(δ) para cualquier $\mathcal{Y}$ de P existe en K los elementos a_1, b_1 tales como $\mathcal{Y} = a_1 \odot b_1^{-1}$.

Defínase la *relación* h de la manera siguiente:

(1) $h(a \cdot b^{-1}) = a \odot b^{-1}$ para cualquier a, b de K.

Muéstrese que h es una aplicación de F en P. Es necesario demostrar que la igualdad (1) define el único valor $h(x)$ que no depende de la representación concreta del elemento x bajo la forma de $x = a \cdot b^{-1}$. En efecto, si $x = c \cdot d^{-1} (c, d \in K)$ es otra representación cualquiera de esta forma del elemento x, entonces $a \cdot b^{-1} = c \cdot d^{-1}$. Por lo tanto, conforme a $(\alpha) a \cdot d = b \cdot c$. Conforme a (γ), se deduce que $a \odot b^{-1} = c \odot b^{-1}$. Así,

$h(a \cdot b^{-1}) = a \odot b^{-1} = c \odot d^{-1} = h(c \cdot d^{-1})$.

Así, se estableció que h es una aplicación (función). Conforme a (1) y de la condición (β) $\mathrm{Dom}\, h = F$. Conforme a (1) y la condición (δ) $\mathrm{Im}\, h = P$. Por tanto, h es una aplicación del conjunto F sobre P.

Una verificación directa demuestra que h es un homomorfismo del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$, es decir para cualquier x, y de F satisfacen las condiciones

$$h(x + \mathcal{Y}) = h(x) \oplus h(\mathcal{Y}),\ h(-x) = \ominus h(x),\ h(x \cdot \mathcal{Y})\, h(x) \odot h(\mathcal{Y}), h(1_{\mathcal{F}}) = 1_{\mathcal{P}}.$$

La aplicación h es inyectiva. En efecto, si para los elementos $a \cdot b^{-1}$ y $c \cdot d^{-1}$ de F, se tiene

(2) $h(a \cdot b^{-1}) = h(c \cdot d^{-1})$,

entonces, según (1) en el cuerpo $\mathcal{P}$ se verifica la igualdad $a \odot b^{-1} = c \odot d^{-1}$. Conforme a (δ), se deduce la igualdad $a \cdot d = b \cdot c$. Conforme a (α) de la última igualdad se deduce que

(3) $a \cdot b^{-1} = c \cdot d^{-1}$.

En resumen, se estableció que, para cualquier elemento $a \cdot b^{-1}$ y $c \cdot d^{-1}$ del conjunto F, de (2) se deduce (3). h es por lo tanto una aplicación inyectiva. Además, h es un homomorfismo. Por tanto, h es un isomorfismo del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$. Finalmente, conforme a (1), $h(a) = a$ para cualquier a de K, es decir h hace pasar cada elemento del anillo $\mathcal{K}$ en el mismo. □

Ejercicios

1. Sean $\mathcal{K}$ un sub-anillo del cuerpo $\mathcal{F}$ y K su conjunto de base. Sea $\mathcal{P}$ un sub-cuerpo del cuerpo $\mathcal{F}$ generado por el conjunto K, es decir $\mathcal{P}$ es la intersección de todos los sub-cuerpos $\mathcal{F}$ que contienen el conjunto K. Demostrar que $\mathcal{P}$ es un cuerpo de los cocientes del anillo $\mathcal{K}$.
2. Sean $\mathbb{Z}[i] = \{m + ni | m, n \in \mathbb{Z}\}$ y $z[i]$ un sub-anillo del cuerpo de los números complejos con conjunto de base $\mathbb{Z}[i]$. Sean $Q(i) = \{a + bi | a, b \in Q\}$ y $Q(i)$ un sub-cuerpo de los números complejos en conjunto de base $Q(i)$. mostrar que $Q(i)$ es un cuerpo de los cocientes del anillo $z[i]$.
3. Sean $\mathcal{P}$ y $\mathcal{P}'$ cuerpos de los cocientes de los dominios de integridad $\mathcal{K}$ y $\mathcal{K}'$ respectivamente y h un isomorfismo de $\mathcal{K}$ sobre $\mathcal{K}'$. Demostrar que existe Un isomorfismo único del cuerpo $\mathcal{P}$ y $\mathcal{P}'$ que prolonga el isomorfismo h.
4. Sean $\mathcal{P}$ un cuerpo de cocientes del dominio de integridad $\mathcal{K}$ y φ un monomorfismo de $\mathcal{K}$ en el cuerpo $\mathcal{F}$. Demostrar que φ puede ser prolongado y eso de manera única hasta el monomorfismo del cuerpo $\mathcal{P}$ en el cuerpo $\mathcal{F}$.

§ 3. Anillos de ideales principales

Propiedades elementales de la divisibilidad en un anillo conmutativo. Sean $\mathcal{K}$ un anillo conmutativo y a, b sus elementos.

DEFINICIÓN. El elemento b se denomina *divisor de* a y el elemento a *múltiplo de* b si existe en $\mathcal{K}$ un elemento c tal como $a = bc$.

La notación $b \mid a$ traduce que b es un divisor de a. La notación $a \vdots b$ demuestra que a es divisible por b o bien que a es múltiplo de b.

El elemento c se llama *divisor común* de a y b si $c \mid a$ y $c \mid b$ (o $a \vdots c$ y $b \vdots c$). De manera análoga, se define el divisor común de muchos elementos de un anillo.

Los elementos a y b del anillo $\mathcal{K}$ se denominan *asociados* en $\mathcal{K}$ si $a \mid b$ y $b \mid a$.

El elemento a se denomina *inversible* en $\mathcal{K}$ o *divisor de unidad* si existe en $\mathcal{K}$ un elemento b tal como $ab = 1$; en ese caso se escribe $b = a^{-1}$.

Un divisor de la unidad divide cualquier elemento del anillo. Si $\mathcal{K}$ es un cuerpo, entonces cualquier elemento de este último es inversible si es diferente de cero.

Estúdiese las propiedades elementales de la divisibilidad en un anillo conmutativo.

PROPOSICIÓN 3.1. *La relación de divisibilidad en un anillo es reflexiva y transitiva, es decir es una relación de pre orden.*

PROPOSICIÓN 3.2. *Un divisor común de dos o varios elementos de un anillo es un divisor de su suma y de su producto.*

PROPOSICIÓN 3.3. *Si el elemento c divide al menos uno de los elementos $a_1, \dots, a_n$, se dividen entonces el producto de esos elementos.*

PROPOSICIÓN 3.4. *Una relación asociativa en un anillo conmutativo es una relación de equivalencia.*

PROPOSICIÓN 3.5. *Si a se asocia a b y $b \mid c$, entonces $a \mid c$.*

La demostración de las proposiciones 3.1-3.5 se dejan al criterio del lector.

PROPOSICIÓN 3.6. *En un dominio de integridad los elementos* a *y* b *se asocian si y solo si existe un elemento* u *inversible en el anillo tal como* $a = ub$.

Demostración. Sea $\mathcal{K}$ un domino íntegro y a, b los elementos asociados en $\mathcal{K}, a \sim b$. Si uno de los elementos a, b es nulo, el otro es obligatoriamente igual a cero. Se tiene entonces $a = 1_{\mathcal{K}} \cdot b$.

Supóngase que $a \sim b$ y $a \neq 0,\ b \neq 0$. Existen entonces los elementos no nulos u y v tales como $a = ub$ y $b = va$. Por tanto, $a = uva$ y $a(uv - 1) = 0$. $\mathcal{K}$ que es un dominio de integridad y $a \neq 0$, se deduce de la última igualdad que $uv - 1 = 0$ y $uv = 1$. Así, el elemento u es inversible en $\mathcal{K}$ y $a = ub$.

Admítase ahora que $a = \varepsilon b$, donde ε es un elemento inversible del anillo $\mathcal{K}$; entonces $b = \varepsilon^{-1}a$. Por tanto, a y b se asocian en $\mathcal{K}$. □

PROPOSICIÓN 3.7. *Sea* A *el conjunto de todos los elementos invertibles del anillo conmutativo* $\mathcal{K}, \mathcal{K} = \langle K, +, -, \cdot, 1\rangle$. *En ese caso el algebra* $\langle A, \cdot, ^{-1} \rangle$, *donde* $^{-1}$ *es una operación singular que asocia al elemento* a *de* A *el elemento inverso* a^{-1}, *es un grupo.*

La demostración de la proposición 3.7 se deja al criterio del lector.

Elementos simples y compuestos de un dominio de integridad. Sea $\mathcal{K}$ un dominio de integridad. Cualquier elemento a del anillo es divisible por cualquier elemento inversible del anillo (para cualquier divisor unidad del anillo) así que para cada elemento asociado en a del anillo. Esos divisores se denominan *divisores triviales del elemento* a.

DEFINICIÓN. Se llama *divisor propio del elemento* a cualquier divisor no trivial de a, es decir un divisor no asociado en a e irreversible en el anillo $\mathcal{K}$.

DEFINICIÓN. Un elemento del dominio de integridad $\mathcal{K}$ se denomina *compuesto* o *reducible en* $\mathcal{K}$ si es diferente de cero y si se puede representar bajo la forma de un producto de dos elementos irreversibles del anillo $\mathcal{K}$.

En otras palabras un elemento del dominio de integridad se denomina *compuesto* si es diferente de cero y si puede representarse bajo la forma de producto de dos divisores propios.

DEFINICIÓN. Un elemento del dominio de integridad $\mathcal{K}$ se denomina *simple* o *irreducible* en $\mathcal{K}$ si es diferente de cero, irreversible y tan sólo admite divisores triviales.

Nótese que cualquier cuerpo es privado tanto de elementos simples como elementos compuestos.

Ejemplos. 1. En un anillo $\mathcal{Z}$ de los enteros el elemento p diferente de 0 y de ± 1 es un elemento simple si y sólo si sus divisores tan solo son los elementos $\pm 1,\ \pm p$. En el anillo $\mathcal{Z}$ los números $\pm 2, \pm 3, \pm 5, \ldots$ son simples (o primos).

2. En el anillo $\mathcal{Z}$, 6 es un elemento compuesto, ya que $6 = 2 \cdot 3$ y $2,\ 3$ son elementos irreversibles.

El conjunto de todos los elementos de un dominio de integridad se divide en cuatro clases: $1)$ el conjunto que consta de un elemento cero; $2)$ el conjunto de todos los elementos inversibles (el conjunto de todos los divisores de unidad); $3)$ el conjunto de todos los elementos simples (primos); $4)$ el conjunto de todos los elementos compuestos. Las dos últimas clases pueden ser vacías (si el dominio de integridad es un cuerpo).

TEOREMA 3.8. *Sean* $\mathcal{K}$ *un dominio de integridad,* $a, b \in K$ *y* 1 *el elemento unidad del anillo* $\mathcal{K}$. *Entonces:*

(1) $b \mid a$ *si y sólo si* $(a) \subset (b)$;
(2) $a \mid 1$ *si y sólo si* $(a) = (1)$;
(3) $a \sim b$ *si y sólo si* $(a) = (b)$;
(4) *si* b *es un divisor propio de* a, *entonces* $a \overset{\subset}{\neq} (b)$;
(5) $a \overset{\subset}{\neq} (b)$ *si y solo si* $b \mid a$ *y* a *no divide* b.

Demostración. (1) Sea $b \mid a$, es decir que existe un elemento c de K tal que $a = bc$; entonces $a \in (b)$;

$$(a) = \{ma | m \in K\} = \{mcb | m \in K\} \subset \{lb | l \in K\} = (b)$$

y, por consiguiente, $(a) \subset (b)$. Admítase ahora que $(a) \subset (b)$; entonces $a \in (b)$ y, por consiguiente, $a = bc$ para determinada c de K, $i.e.$ $b|a$;

(2) si $a \mid 1$, entonces $(1) \subset (a)$, conforme a (1). Además, $(a) \in (1)$, dado que $(1) = K$; así, $(a) = (1)$. Si $(a) = (1)$, se tiene entonces $a \mid 1$, conforme a (1);

(3) Si $a \sim b$, es decir $a \mid b$ y $b \mid a$, entonces, conforme a (2), $(b) \subset (a)$ y $(a) \subset (b)$ y, por consiguiente, $(a) = (b)$. Si $(a) = (b)$, entonces $a \in (b)$ y $b \in (a)$, y así, $b \mid a$ y $a \mid b$, por tanto, $a \sim b$;

(4) supóngase que b es un divisor propio de a, es decir $b \nsim 1$, $b \nsim a$ y $b \mid a$. Entonces, conforme a (1) y (3), $(b) \neq (a)$ y $(a) \subset (b)$, y, por consiguiente, $a \underset{\neq}{\subset} (b)$;

(5) Si $a \underset{\neq}{\subset} (b)$, entonces, conforme a (1), $b \mid a$ y, conforme a (3), $a \nsim b$ y, por consiguiente, $b \nmid a$. La recíproca se deduce de (1) y (3). □

Anillos de ideales principales. Es necesario despejar y estudiar en la clase de los dominios de integridad los anillos de los cuales cada ideal sea principal.

DEFINICIÓN. Se llama *anillo de ideales principales o anillos principales* al dominio de integridad de los cuales cada ideal es el ideal principal.

Ejemplos. 1. Cualquier cuerpo es un anillo de ideales principales.

2.El anillo Z de los enteros es un anillo de ideales principales.

Recuérdese que el conjunto $(a, b) = \{ax + bY | x, Y \in K\}$, donde a, b son elementos fijos en K, es un ideal de un anillo conmutativo $\mathcal{K}$.

Estúdiese las propiedades de los anillos de ideales principales.

PROPOSICIÓN 3.9. *Sean p un elemento simple del anillo $\mathcal{K}$ de ideales principales y $a \in K$. Si p no divide a, entonces $(p, a) = (1)$.*

Demostración. Por hipótesis, cada ideal del anillo $\mathcal{K}$ es principal. Así, existe en $\mathcal{K}$ un elemento c tal que $(p, a) = (c)$. El elemento c divide los elementos p y a:

(1) $c \mid p$, $c \mid a$.

Dado que c es un divisor del elemento simple $p, c \sim p$ o c divide 1. Si $c \sim p$, entonces $p \mid c$ y pues conforme a (1) $c \mid a$, se tiene $p \mid a$, lo que es en contradicción con la hipótesis. Por lo tanto, c divide 1. Por consiguiente, $(c) = (1)$ y $(p, a) = (1)$. □

PROPOSICIÓN 3.10. *Sean p un elemento simple del anillo $\mathcal{K}$ de ideales principales y $a, b \in K$. Si p divide ab, entonces p divide igualmente a o b.*

Demostración. Si p no divide a, entonces, conforme a la proposición 3.9, $(p, a) = (1)$. Existe por lo tanto en K los elementos u, v tales que $up + va = 1$. Al multiplicar los dos miembros de la igualdad por b, resulta que $upb + vab = b$. Por lo tanto, si p divide ab, divide igualmente $upb + vab$ y b. Así, si $p \nmid a$, entonces $p \mid b$. □

PROPOSICIÓN 3.11. *Sean p un elemento simple del anillo $\mathcal{K}$ de ideales principales y $a_1, \dots, a_n \in K$. Si p divide el producto $a_1 a_2, \dots, a_n$, entonces divide uno o menos factores $a_1, \dots, a_n$.*

La demostración de esta proposición se efectúa por inducción sobre n apoyándose sobre la proposición 3.10.

DEFINICIÓN. La sucesión $(a_1), (a_2), (a_3), \dots$ de ideales principales de un anillo se denomina *cadena ascendente de ideales* si

(1) $(a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} (a_3) \underset{\neq}{\subset} \dots$

PROPOSICIÓN 3.12. *En un anillo de ideales principales una cadena ascendente de ideales no puede ser infinita.*

Demostración. Sea (1) la cadena ascendente del anillo $\mathcal{K}$ de ideales principales. Nótese I la reunión de todos los ideales de la cadena (1), es decir

(2) $I = \bigcup_i (a_i)$.

Una verificación directa demuestra que el conjunto I esta cerrado respecto a la substracción y estable respecto a la multiplicación por los elementos del anillo $\mathcal{K}$. I es por lo tanto un ideal del anillo $\mathcal{K}$ y, además, un ideal principal. Existe por lo tanto en $\mathcal{K}$ un elemento c tal que $I = (c)$. Apoyándose sobre (2) búsquese un índice m tal que $c = \in (a_m)$. $c = \in (a_m)$ y $a_m \in I = (c)$, se tiene $I = (a_m) = (c)$. Por lo tanto, el ideal (a_m) es el último eslabón de la cadena (1). □

Anillo factorial de los ideales principales. Se propone generalizar a los anillos de ideales principales el TEOREMA de la existencia y unicidad de la factorización de elementos del anillo $\mathcal{Z}$ de enteros.

DEFINICIÓN. Se denomina que un elemento a del dominio de integridad $\mathcal{K}$ admite una factorización única si se cumplen las condiciones siguientes:

(1) existe en $\mathcal{K}$ elementos simple (primos) p_i tales que

$$a = \prod_{i=1}^{m} p_i ;$$

(2) si $a = \prod_{i=1}^{n} q_i ;$ es otra factorización, donde q_i son elementos simples de $\mathcal{K}$, entonces $m = n$ y para una numeración adecuada $p_i \sim q_i$ para $i = 1, \dots, m$.

DEFINICIÓN. El anillo $\mathcal{K}$ se denomina *factorial* (con factorización única) si este es un dominio de integridad y cualquier elemento del anillo diferente de cero e irreversible se descompone en factores primos.

Nótese que cualquier cuerpo es un anillo factorial dado que no posee elemento irreversible diferente de cero.

TEOREMA 3.13. *Un anillo de ideales principales es un anillo factorial.*

Demostración. Sea $\mathcal{K}$ un anillo de ideales principales. Es necesario demostrar que cualquier elemento irreversible diferente de cero del anillo se descompone en factores primos. Supóngase que existe $\mathcal{K}$ un elemento irrevertible no nulo a no se puede descomponer en factores primarios en $\mathcal{K}$. El elemento a es entonces un elemento compuesto. Por lo tanto se puede representar bajo la forma de un producto de dos divisores propios $a = a_1 b$ y, según el punto (4) del TEOREMA 3.8, $(a) \overset{\subset}{\neq} (a_1)$.

Uno o menos factores $a_1, b_1,$ por ejemplo $a_1,$ no se descomponen en factores primos. Se puede así representar a_1 bajo forma de producto de dos factores propios:

$$a_1 = a_2 b_2, \quad (a_1) \overset{\subset}{\neq} (a_2),$$

Etc. Así, existe una cadena ascendente infinita

$$(a) \overset{\subset}{\neq} (a_1) \overset{\subset}{\neq} (a_2) \overset{\subset}{\neq} \dots$$

de ideales del anillo $\mathcal{K}$, lo que es posible conforme a la proposición 3.12. po lo tanto, cualquier elemento irreversible diferente a cero del anillo $\mathcal{K}$ se descompone en factores primos.

Demuéstrese que esta factorización es única. Si a es un elemento simple, entonces el TEOREMA se cumple. Supóngase que el TEOREMA se cumple en los elementos representados bajo la forma de producto de n factores primos y demuéstrese que también se cumple en los elementos representables bajo la forma de producto de $n + 1$ factores primos. Sean dadas dos descomposiciones cualquieras del elemento a en factores primos:

$$(1)\ a = p_1 \dots p_n p_{n+1} = q_1 \dots q_s q_{s+1}.$$

El elemento simple p_{n+1} divide el producto $q_1 \dots q_{s+1}$. Por tanto, la proposición 3.14, divide al menos uno de los factores $q_1, \dots, q_{s+1},$ por ejemplo $q_{s+1} \cdot p_{n+1}$ y q_{s+1} que son números primos, se tiene $q_{s+1} = u p_{n+1},$ donde u es un elemento inversible del anillo. Al simplificar los dos miembros de la igualdad (1) por $p_{n+1},$ se tiene

$$p_1 \dots p_n = q_1 \dots (u q_s).$$

Por lo tanto, por hipótesis de inducción $n = s$ y para una numeración adecuada $p_i \sim q_i$ para $i = 1, \dots, n$. Además, $p_{n+1} \sim q_{n+1}$. El razonamiento por inducción se concluyó. □

Anillos euclidianos. Sean $\mathbf{N}$ el conjunto de todos los números naturales, K el conjunto de base del anillo $\mathcal{K}$.

DEFINICIÓN. Un dominio integro $\mathcal{K}$ se denomina *anillo euclidiano* si existe una aplicación h del conjunto K en $\mathbb{N}$ que satisfacen las condiciones:

(α) para cualquier a, b de K con $b \neq 0$ existe en K elementos q, r tales que $a = bq + r$ y $h(r) < h(b)$;

(β) para cualquier a de K la igualdad $h(a) = 0$ es verdadera si y sólo si $a = 0$.

Ejemplo. Sea h una aplicación del conjunto K de los enteros en $\boldsymbol{N}$ por la cual $h(a) = |a|$. Conforme al TEOREMA de la división con resta (ver TEOREMA 4.4.4), h cumplió las condiciones (α) y (β). Por lo tanto, $\mathcal{Z}$ es un anillo euclidiano.

TEOREMA 3.14. *Un anillo euclidiano es un anillo de ideales principales.*

Demostración. Sean $\mathcal{K}$ un anillo euclidiano y h la aplicación del conjunto K en $\mathbb{N}$ que satisface a las condiciones (α) y (β). El ideal nulo es aparentemente el ideal principal. Sea M un ideal no nulo del anillo $\mathcal{K}$. Se debe demostrar que M es un ideal principal. Dado que $M \setminus \{0\}$ es un conjunto no vacío, conforme a (β), $h(M \setminus \{0\})$ es un sub-conjunto no vacío del conjunto $\mathbb{N} \setminus \{0\}$ y, por consiguiente, según el TEOREMA 4.3.11, $h(M \setminus \{0\})$ contienen el más pequeño elemento. Por consiguiente, existe en M un elemento no nulo b tal que

(1) $h(b) \leq h(x)$ para cualquier (x) de $M \setminus \{0\}$.

Demuéstrese que $M = (b)$. Sea a un elemento cualquiera del conjunto $M \setminus \{0\}$. Conforme a la condición (α), existe en K los elementos q y r tales que

(2) $a = bq + r$ y $h(r) < h(b)$.

Dado que M es un ideal y $a, b \in M$, se tiene $r = a - bq \in M$ y, conforme a (1), (2) resulta

(3) $r \notin M \setminus \{0\}$.

Por lo tanto, $r = 0$ y $a = bq$. Ahora bien, como a es un elemento no nulo cualquiera del conjunto $M, M \subset (b)$. Dado que $b \in M$, se tiene $M = (b)$; por consiguiente, cualquier ideal del anillo euclidiano $\mathcal{K}$ es un ideal principal. □

Corolario 3.15. *Cualquier anillo euclidiano es un anillo factorial.*

Corolario 3.16. *Un anillo $\mathcal{Z}$ de los enteros es un anillo de ideales principales y, por tanto, un anillo factorial.*

Ejemplo. Sea $\mathbf{Z}[i] = \{m + ni | m, n \in \boldsymbol{Z}\}$. El conjunto $\boldsymbol{Z}[i]$ está cerrado en el anillo $\mathcal{C}$ de números complejos. Por tanto, el algebra $\mathbf{Z}[i] = \langle \mathbf{Z}[i], +, -, \cdot, 1 \rangle$ es un sub-anillo del anillo $\mathcal{C}$. Este anillo se denomina *anillo de enteros gaussianos.* Muéstrese que el anillo $\mathbf{Z}[i]$ es euclidiano. Considérese la aplicación h del conjunto $\mathbf{Z}[i]$ en $\mathbf{N}$ por la cual, para $a = m + ni, h(a) = |a|^2 = m^2 + n^2$. La condición (β) aparentemente se cumple. Se mostraría que para h se cumple la condición (α). Sean $a, b \in \mathbf{Z}[i]$ y $b \neq 0$. Entonces $a/b = \sigma + \tau i$, donde $\sigma, \tau \in \mathbf{Q}$. Existen enteros s y t tales que $|s - \sigma| \leq \frac{1}{2}$ y $|t - \tau| \leq \frac{1}{2}$. Supóngase $\alpha = \sigma - s$ y $\beta = \tau - t$. Entonces, $a = b(s + \alpha + (t + \beta)i) = bq + r$, donde $q = s + ti$ y $r = b(\alpha + \beta i)$; además, $q = s + ti \in \mathbf{Z}[i]$ y $r = a - bq \in \mathbf{Z}[i]$. Por lo tanto, $h(r) = |r|^2 = |b|^2(\alpha^2 + \beta^2) \leq \frac{1}{2}|b|^2 = \frac{1}{2}h(b)$ y $h(r) < h(b)$, es decir h satisface igualmente a la condición (α). Así, el anillo de enteros gaussianos es un anillo euclidiano.

Ejercicios

1. Sean K un conjunto de todos los números racionales m/n en denominadores impares n y $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un sub-anillo del cuerpo Q de los números racionales. Mostrar que $\mathcal{K}$ es un anillo de ideales principales.
2. Sea $\mathcal{Z}[i]$ un anillo de enteros gaussianos. Buscar los elementos invertibles de este anillo.
3. Demostrar que un anillo cociente $\mathcal{Z}[i]/(3)$ del anillo de enteros gaussianos que siguen el ideal (3) es un cuerpo que contiene nueve elementos.
4. Demostrar que el anillo cociente $\mathcal{Z}[i]/(n)$ del anillo de enteros gaussianos (n) es un cuerpo si y sólo si n es un número primo no igual a la suma de cuadrados de dos enteros.
5. Sean $K = \{a + bi\sqrt{3}\,|a, b \in \mathcal{Z}\}$ y $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un sub-anillo de un cuerpo de números complejos. Mostrar que en el anillo $\mathcal{K}$ cualquier elemento irreversible diferente de cero se descompone en factores primos, pero no siempre unívocamente. En particular, mostrar que $4 = 2.2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ son dos descomposiciones de 4 en producto de factores primos, 2 no están asociados a $1 \pm i\sqrt{3}$.
6. Sea K un conjunto de todos los números complejos de la forma $a + ib\sqrt{3}$, donde a y b son ya enteros, o ambos mitades de enteros impares. Sea $\mathcal{K}$ un sub-anillo de un cuerpo de números complejos en conjunto de base K. Demostrar que el anillo $\mathcal{K}$ es euclidiano.
7. Demostrar que el elemento p del anillo $\mathcal{K}$ de ideales principales es simple (primo) si y sólo si el anillo cociente $\mathcal{K}/(p)$ es un dominio integro.
8. Sean $\mathrm{Z}[\sqrt{2}] = \{m + n\sqrt{2}|m, n \in \mathbf{Z}\}$ y $\mathcal{Z}[\sqrt{2}]$ un sub-anillo de un cuerpo de números reales en conjunto de base $\mathbb{Z}[\sqrt{2}]$. Demostrar que el anillo $\mathcal{Z}[\sqrt{2}]$ es euclidiano.

§ 4. Máximo común divisor. Mínimo común múltiplo.

Máximo común divisor. Sea $\mathcal{K}$ un anillo conmutativo. El elemento c se denomina *divisor de los elementos* $a_1, \dots, a_m$ del anillo $\mathcal{K}$ si c es un divisor (en $\mathcal{K}$) de cada uno de esos elementos.

DEFINICIÓN. Se llama *máximo común divisor de los elementos* $a_1, \dots, a_m$ del anillo $\mathcal{K}$ su máximo común divisor divisible por cualquier divisor de esos elementos.

El máximo común divisor de los elementos $a_1, \dots, a_n$ se denota MCD $a_1, \dots, a_n$.

De la definición antes mencionada se deriva la proposición siguiente.

PROPOSICIÓN 4.1. *Si d es el máximo común divisor de los elementos $a_1, \dots, a_n$ en $\mathcal{K}$, el conjunto de todos los divisores comunes de los elementos $a_1, \dots, a_n$ coincide con el conjunto de todos los divisores del elemento d.*

DEFINICIÓN. Los elementos a y b del anillo $\mathcal{K}$ se denominan *primos entre ellos* si la unidad (divisor unidad) del anillo $\mathcal{K}$ es su máximo común divisor en $\mathcal{K}$.

Se estudia más adelante las propiedades del máximo común divisor en el anillo de ideales principales. La proposición 4.2 es aplicable a cualquier anillo conmutativo.

PROPOSICIÓN 4.2. *Los dos máximos comunes divisores de los elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$ son asociados a $\mathcal{K}$. Si c es el máximo común divisor de los elementos $a_1, \dots, a_n$ si bien asociados a d, entonces d es igualmente el máximo común divisor de esos elementos.*

Esta propiedad resulta directamente de la definición del máximo común divisor.

PROPOSICIÓN 4.3. *Para cualquier colección de elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$ de ideales principales existe un máximo común divisor en $\mathcal{K}$. El elemento d es el máximo común divisor de los elementos $a_1, \dots, a_n$ si y solo si* $(a_1, \dots, a_n) = (d)$.

Demostración. Supóngase que

$$(1)\quad (a_1, \dots, a_n) = (d),$$

y demuéstrese que d es MCD $(a_1, \dots, a_n)$. Se deduce de (1) que d es un común divisor de los elementos $a_1, \dots, a_n$ y se tiene:

$$(2)\quad d = \lambda_1 a_1 + \cdots + \lambda_n a_n, \text{ donde } \lambda_1, \dots \lambda_n \in K.$$

Además, conforme a (2), si c es el divisor común de $a_1, \dots, a_n$, entonces c divide d. Por lo tanto, d es MCD $(a_1, \dots, a_n)$.

Supóngase ahora que d es MCD $(a_1, \dots, a_n)$ y demuéstrese que entonces $(a_1, \dots, a_n) = (d)$. $\mathcal{K}$ es el anillo de ideales principales, existe en K un elemento c tal que $(a_1, \dots, a_n) = (c)$. Como se acaba de demostrar, c es MCD $(a_1, \dots, a_n)$. Conforme a la proposición 4.2, se deduce que c y d están asociados y, por consiguiente, según el TEOREMA 3.8, $(c) = (d)$. Por tanto, $(a_1, \dots, a_n) = (d)$. □

TEOREMA 4.4. *Sea d el divisor común de los elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$ de ideales principales*. El elemento d es MCD $(a_1, \dots, a_n)$ *si y sólo si puede ser representado bajo la forma de* $d = \lambda_1 a_1 + \cdots + \lambda_n a_n$ *donde* $\lambda_1, \dots, \lambda_n \in K$.

Demostración. Sea d MCD $(a_1, \dots, a_n)$. Entonces, según la proposición 4.3, $(d) = (a_1, \dots, a_n)$ .por lo tanto, se puede representar d bajo la forma de $d = \lambda_1 a_1 + \cdots + \lambda_n a_n$, donde $\lambda_1, \dots \lambda_n \in K$.

Supóngase ahora que d puede representarse bajo la forma de $d = \lambda_1 a_1 + \cdots + \lambda_n a_n, \lambda_i \in K$. Entonces, cualquier divisor común c de los elementos $a_1, \dots, a_n$ divide la suma $\lambda_1 a_1 + \cdots + \lambda_n a_n$, y, por tanto, divide d. Por consiguiente, d es el máximo común divisor de los elementos $a_1, \dots, a_n$. □

PROPOSICIÓN 4.5. *Para cualquier elemento $a_1, \dots, a_n$ y el divisor común c del anillo $\mathcal{K}$ de ideales principales, se tiene*

$$\text{MCD}\,(ca_1, \dots, ca_n) \sim c \cdot \text{MCD}\,(a_1, \dots, a_n).$$

Demostración. Sea d MCD $(a_1, \dots, a_n)$. Según el TEOREMA 4.4, existe en K los elementos $\lambda_1, \dots, \lambda_n$ tales que $d = \lambda_1 a_1 + \cdots + \lambda_n a_n$. por lo tanto $cd = \lambda_1(ca_1) + \cdots + \lambda_n(ca_n)$. Además, dado que d es el divisor común de $a_1, \dots, a_n, cd$ es también un divisor común de $ca_1, \dots, ca_n$. Por consiguiente, según el TEOREMA 4.4, cd es el máximo común divisor de los elementos $ca_1, \dots, ca_n$. □

PROPOSICIÓN 4.6. *Si d es el máximo común divisor de los elementos a y b en el anillo $\mathcal{K}$ de ideales principales y $d \neq 0$ entonces, los elementos a/d y b/d son primos entre ellos.*

Demostración. Por hipótesis, MCD $(\mathrm{a}, \mathrm{b}) = \mathrm{d} \neq 0$. Según el TEOREMA 4.4, se deduce que $\lambda_1 \mathrm{a} + \lambda_2 \mathrm{b} = \mathrm{d}$ para ciertas $\lambda_1 \lambda_2 \in \mathrm{K}$; también, $\lambda_1 \frac{\mathrm{a}}{\mathrm{d}} + \lambda_2 \frac{\mathrm{b}}{\mathrm{d}} = 1$. Según el TEOREMA 4.4, se deduce que 1 es el máximo común divisor de los elementos a/d y b/d, y, por tanto, que los elementos a/d y b/d son primos entre ellos. □

La proposición 4.6 puede aparentemente ser generalizada de la manera siguiente: si d es el máximo común divisor de los elementos $a_1, \dots, a_n$ en el anillo $\mathcal{K}$ de ideales principales y $\mathrm{d} \neq 0$, entonces 1 es el máximo común divisor de los elementos $a_1/d, \dots, a_n/d$.

TEOREMA 4.7. *Si en el anillo de ideales principales a divide bc y los elementos a, b son primos entre ellos, entonces a divide c*.

Demostración. Por hipótesis, MCD $(a, b) = 1$. Según el TEOREMA 4.4, se deduce que $\lambda_1 \mathrm{a} + \lambda_2 \mathrm{b} = 1$ para ciertas $\lambda_1, \lambda_2 \in K$. Al multiplicar los dos miembros de la igualdad por c, se obtiene $\lambda_1 \mathrm{ac} + \lambda_2 \mathrm{bc} = \mathrm{c}$. Dado que, por hipótesis, a divide bc, también divide $\lambda_1 \mathrm{ac} + \lambda_2 \mathrm{bc}$ y, por tanto, a divide c. □

Mínimo común múltiplo: Sea $\mathcal{K}$ un anillo de ideales principales. Al elemento c se conoce como *múltiplo común de los elementos $a_1, \dots, a_n$* del anillo $\mathcal{K}$ si c se divide en $\mathcal{K}$ por cada uno de esos elementos.

DEFINICIÓN. Se denomina *mínimo común múltiplo de los elementos $a_1, \dots, a_n$* del anillo $\mathcal{K}$ al múltiplo común que divide a todo múltiplo común de esos elementos.

Un mínimo común múltiplo de elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$ se denota $M.C.M.(a_1, \dots, a_n)$.

De esta definición se deriva directamente la proposición siguiente:

PROPOSICIÓN 4.8: *Si m es el mínimo común múltiplo de elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$, el conjunto de todos los múltiplos comunes de elementos $a_1, \dots, a_n$ coincide entonces con el conjunto de todos los múltiplos de elemento m.*

Estúdiese las propiedades de un mínimo común múltiplo en el anillo $\mathcal{K}$ de ideales principales. La proposición 4.9 se aplica a todo anillo conmutativo.

PROPOSICIÓN 4.9: Cualquiera de los dos mínimo común múltiplos de elementos $a_1, \dots, a_n$ del anillo $\mathcal{K}$ están asociados en $\mathcal{K}$. Si m es el mínimo común múltiplo de los elementos $a_1, \dots, a_n$ y m está asociado a m', entonces m'es también un mínimo común múltiplo de elementos $a_1, \dots, a_n$.

Esta proposición se deriva directamente de la definición del mínimo común múltiplo.

PROPOSICIÓN 4.10: *Un elemento m es el mínimo común múltiplo de los elementos del anillo $\mathcal{K}$ si y sólo si*

$(a_1) \cap (a_2) \cap \dots \cap (a_n) = (m)$.

Demostración. Supóngase que

(1) $(a_1) \cap \dots \cap (a_n) = (m)$.

Entonces m es un múltiplo común de los elementos $a_1, \dots, a_n$. Ademas,Si m' es un múltiplo común de los elementos $a_1, \dots, a_n$, entonces

$m' \in (a_1), \dots, m' \in (a_n)$, es decir

$$m' \in (a_1) \cap \dots \cap (a_n) = (m)$$

Y, por lo tanto, m' es múltiplo de m. Por consiguiente, m es el mínimo común múltiplo de los elementos $a_1, \dots, a_n$.

Supóngase que m es el $\mathrm{M.C.M}(a_1, \dots, a_n)$. Siendo $\mathcal{K}$ un anillo de ideales principales, en $\mathcal{K}$ existe un elemento m_1 tal que

$(a_1) \cap \dots \cap (a_n) = (m_1)$.

Según esta demostración m_1 es el mínimo común múltiplo de los elementos $a_1, \dots, a_n$. Como resultado de la proposición 4.9, $m_1$está asociado a m. Por consiguiente,

$(m_1) = (m)$ y $(a_1) \cap \dots \cap (a_n) = (m)$. □

COROLARIO 4.11: *Para toda serie $a_1, \dots, a_n$ de elementos del anillo $\mathcal{K}$ existe un Mínimo común múltiplo en $\mathcal{K}$.*

PROPOSICIÓN 4.12: *Para todos los elementos a, b, c del anillo $\mathcal{K}$.*

(1) $\mathrm{M.C.M}(ac, bc) \sim c.\ \mathrm{M.C.M}(a, b)$.

Demostración. Sea m un $\mathrm{M.C.M}(a, b)$. Se debe demostrar que mc es un $\mathrm{M.C.M}(ac, bc)$. Es ciertamente verdadero para $c = 0$. Supóngase que $c \neq 0$. Siendo m un múltiplo común de a y b, mc lo es de ac y bc. Sea m' cualquier múltiplo común de elementos ac y bc, es decir

(2) $m' = kac,\ m' = sbc, o\ \ k, \mathcal{S} \in K$.

Ya que $\mathcal{K}$ es un dominio de integridad y $c \neq 0$, de $\mathcal{K}ac = \mathcal{S}bc$ se deduce que $ka = sb$. Por lo tanto, ka es múltiplo de m, quiere decir que $ka = rm, \text{donde } r \in K$. Por tanto, en virtud de (2), $m' = rmc$ y, por tanto, m'es múltiplo de mc. Asi mc es un $\boldsymbol{M.C.M}$ (ac, bc) y, según la proposición 4.9, el $M.C.M\ (ac, bc) \sim cm$. □

PROPOSICIÓN 4.13: *Si a y b son elementos primos entre sí del anillo $\mathcal{K}$, entonces ab es un mínimo común múltiplo de elementos a ,b.*

Demostración. Sea m un múltiplo común cualquiera de a y b. Demuéstrese que m es múltiplo de ab. Dado que m es múltiplo de b, se tiene $m = bc$, donde $c \in K$. Ya que a divide a m y, por hipótesis, a y b son primos entre sí en $\mathcal{K}$, a divide a c
(Ver el TEOREMA 4.7). Por lo tanto, ab divide a bc y, por consiguiente , m es múltiplo de ab.Por tanto, ab es el minimo común múltiplo de los elementos a, b. □

PROPOSICIÓN 4.14: Si a, b son elementos no nulos del anillo $\mathcal{K}$,

entonces el $M.C.M(a,b) \sim \frac{ab}{M.C.D\ (a,b)}$.

Demostración. Sea d el $\mathrm{M.C.D}\ (a,b)$ en $\mathcal{K}$.Dado que a , b son elementos no nulos, se tiene $d \neq 0$. Según la proposición 4.12:

(1) El $M.C.M(a,b) \sim d.M.C.M\ \left(\frac{a}{d}, \frac{b}{d}\right)$.

Conforme a la proposición 4.6, el $M.C.D\ \left(\frac{a}{d}, \frac{b}{d}\right) = 1$, quiere decir que los elementos $\frac{a}{d}$ y $\frac{b}{d}$ son primos entre sí.

De ahí, según la proposición 4.13, se deduce que

(2) $\mathrm{M.C.M}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{a}{d}.\frac{b}{d}$.

En base a (1) y (2) se concluye que $\mathrm{M.C.M}\ (a,b) \sim \frac{ab}{d}$. □

TEOREMA 4.15*: Sean* $a = u.p_1^{a1}\ldots p_m^{am}, b = v.p_1^{\beta 1}\ldots p_m^{\beta m}$, donde $p_1, \ldots, p_m$ *son elementos irreducibles diferentes dos a dos del anillo factorial* $\mathcal{K}$, u, v *siendo elementos irreducibles del anillo.*
Entonces se tiene:

(1) $M.C.M\ (a\ , b) = p_1^{\gamma 1} \ldots\ p_m^{\gamma m}, donde\ \gamma_i = \max(a_i\ \beta_i)$;

(2) $M.C.D\ \ (a\ , b\ ) = p_1^{\delta 1}\ldots p_m^{\delta m}$, donde $\delta_1 = \min(a_i, \beta_i)$.

La demostración de la formula (1) se esboza de manera análoga a la de la preposición 11.3.8. La demostración de la formula (2) se esboza de manera análoga a la de proposición 11.3.1.

Ejercicios

1. Demostrar el TEOREMA 4.15.
2. Demostrar que el TEOREMA 4.7 y la proposición 4.6 son verdaderas para todo anillo factorial $\mathcal{K}$.
3. Mostrar que las proposiciones 4.10 - 4.14 son verdaderas para todo anillo factorial $\mathcal{K}$.
4. Sean a, b, c elementos de un anillo factorial, $M.C.D\ \ (a\ , c\ ) \sim 1$ y $M.C.D\ \ (b, c) \sim 1$. Demostrar que el $M.C.D\ (ab, c) \sim 1$.
5. Sean $a, b,$ c elementos de un anillo factorial. Demostrar que el $M.C.M\ \big(a, M.C.D(b,c)\big) \sim M.C.D\big(M.C.M\ (a,b), M.C.M(a,c)\big)$.

CAPITULO XIV
POLINOMIOS EN UNA VARIABLE

§ 1. Anillos de polinomios

Extensión transcendente simple del anillo: Sean $\mathcal{K}$ y $\mathcal{L}$ anillos conmutativos en conjuntos de base K y L respectivamente.

DEFINICIÓN. A un anillo $\mathcal{L}$ se le conoce como *extensión simple del anillo* $\mathcal{K}$ por adjunción del elemento u si estas satisfacen las condiciones:

(1) $\mathcal{K}$ es un subanillo del anillo $\mathcal{L}$;

(2) Todo elemento a de L puede representarse bajo la forma

$a = a_0 + a_1^u + \ldots + a_n^{u^n}$, o $a_0, a_1, \ldots, a_n \in K$.

La notación $\mathcal{L} = \mathcal{K}[u]$ significa que el anillo $\mathcal{L}$ es una extensión simple del anillo $\mathcal{K}$ por adjunción del elemento u. En ese caso el conjunto de base del anillo $\mathcal{L}$ es igualmente se denotado $K[u], L = K[u]$.

DEFINICIÓN. Un anillo $\mathcal{L} = \mathcal{K}[u]$ se denominado *extensión trascendente simple del anillo* $\mathcal{K}$ si este satisface la condición siguiente:

(3) Para cualquier elementos $a_0, a_1, \ldots, a_n$ del conjunto K de la igualdad

$a_0 + a_1^u + \ldots + a_n^{u^n} = 0$ Se deducen las igualdades $a_0 = 0, a_1 = 0, \ldots, a_n = 0$.

Si $\mathcal{L} = \mathcal{K}[u]$ es una extensión simple del anillo $\mathcal{K}$ por adjunción de u y u satisface a las condiciones (3), el elemento u se denominado por lo tanto *trascendente con relación a* $\mathcal{K}$.

Si $\mathcal{K}[u]$ es una extensión trascendente simple del anillo $\mathcal{K}$ por adjunción de u, igualmente se denota al anillo $\mathcal{K}[u]$ *anillo de polinomios en u sobre* $\mathcal{K}$ y los elementos del anillo $\mathcal{K}[u]$ *polinomios en u sobre* $\mathcal{K}$ *o polinomios sobre* $\mathcal{K}$.

PROPOSICIÓN 1.1. *Sea* $\mathcal{K}[u]$ *una extensión trascendante simple del anillo* $\mathcal{K}$ *por adjunción de* u. *Entonces para todo elemento a del anillo* $\mathcal{K}[u]$,

Si $a = a_0 + a_1^u + \ldots + a_n^{u^n}$ y $a = a_0' + a_1' u + \ldots + a_1' u^n$, o $a_i, a_i' \in K$, se tiene $a_i = a_i'$ para $i = 1, \ldots, n$.

DEMOSTRACIÓN. Si

$a = a_0 + a_1^u + \ldots + a_n^{u^n}$ y $a = a_0' + a_1' u + \ldots + a_1' u^n$, $(a_i, a_i' \in K)$,

Entonces

(1) $a_0 - a_0' + (a_{1-} a_0') u + \ldots + (a_n - a_n') u^n = 0$.

Por hipótesis, el elemento u es trascendente sobre $\mathcal{K}$. Por lo tanto de (1) se deducen las igualdades $a_i - a_i' = 0$ y $a_i - a_i'$ para $i = 0,1, \ldots, n$. □

TEOREMA 1.2. Sean $\mathcal{K}$ y $\mathcal{L}$ anillos conmutativos, φ un isomorfismo de $\mathcal{K}$ sobre $\mathcal{L}$, mientras que, $\mathcal{K}[x]$ y $\mathcal{L}[y]$ son extensiones trascendentes simples de los anillos $\mathcal{K}$ y $\mathcal{L}$ respectivamente. Entonces $\mathcal{K}[x] \cong \mathcal{L}[\mathrm{y}]$ y existe un único isomorfismo del anillo $\mathcal{K}[x]$ sobre el anillo $\mathcal{L}[\mathrm{y}]$ que hace pasar x en y, prolongando el isomorfismo φ del anillo $\mathcal{K}$ sobre $\mathcal{L}$.

DEMOSTRACIÓN. Desígnese a ψ la aplicación del anillo $\mathcal{K}[x]$en el anillo $\mathcal{L}[\mathcal{Y}]$ definida de la manera siguiente: para toda $a = a_0+\ldots+a_m x^m$ de $K[x]$ se tiene: $\psi(a_0+\ldots+a_m x^m) = \varphi(a_0)+\ldots+\varphi(a_m)y^m$.
Se observa fácilmente que ψ satisface a las condiciones: $\psi(a_0) = \varphi(a_0)$ para todo $a_0\ de\ K, \psi(x) = y$ y $\operatorname{Im}\psi = L[y]$.

A demás, ψ respeta las operaciones principales del anillo $\mathcal{K}[x]$.
Efectivamente, si $a = a_0+\ldots+a_m x^m$ y $b = b_0+\ldots+b_n x^n$ $(m \le n), a, b \in K[x]$, entonces

$$\psi(a+b) = \psi\big((a_0+b_0)+\ldots+(a_m+b_m)x^m + b_m + 1^{x\,m+1}+\ldots+b_{n-1}x^{n-1} + b_n x^n\big) = \varphi(a_0+b_0)+\ldots+\varphi(a_m+b_m)y^m + \varphi(b_{m+1})y^{m+1}+\ldots+\varphi(b_{n-1})y^{n-1} + \varphi(b_n)y^n = (\varphi(a_0)+\ldots+\varphi(a_m)y^m) + (\varphi(b_0)+\ldots+\varphi(b_n)y^n) = \psi(a)+\psi(b).$$

De manera análoga, se puede demostrar que

$$\psi(-a) = -\psi(a), \psi(ab) = \psi(a)\psi(b), \psi(1_{\mathcal{K}}) = 1_{\mathcal{L}}.$$

Por tanto, ψ es un isomorfismo $\mathcal{K}[x]$ sobre $\mathcal{L}$ [y] que hace pasar x en y y prolonga al isomorfismo φ.

Demuéstrese que el isomorfismo de las propiedades ya mencionadas es único. Supóngase que ψ_1 es otro isomorfismo del anillo $\mathcal{K}[x]$ sobre el anillo $\mathcal{L}$ [y] tal que $\psi_1(a_0) = \varphi(a_0)$ con todo a_0 de K y $\psi_1(x) = y$. Por lo tanto, para todo $a = a_0+\ldots+a_m x^m$ de $K[x]$, se tiene:

$$\psi_1(a) = \psi_1(a_0)+\ldots+\psi_1(a_m)\psi_1(x^m) = \varphi(a_0) + \varphi(a_1)y+\ldots+\varphi(a_m)y^m = \psi(a);$$

de este modo, $\psi_1 = \psi$. □

COROLARIO. Sean $\mathcal{K}[x]$ y $\mathcal{K}[y]$dos extensiones trascendentes simples de un anillo conmutativo $\mathcal{K}$. Por lo tanto $\mathcal{K}[x] \cong \mathcal{K}[y]$,y solo existe un isomorfismo del anillo $\mathcal{K}[x]$ sobre el anillo $\mathcal{K}[y]$ haciendo pasar x en y que induce una aplicación idéntica sobre $\mathcal{K}$.

TEOREMA de existencia de la extensión trascendente simple de un anillo conmutativo: Sea $\mathcal{K}$ un anillo conmutativo integro. La serie infinita $a = (a_0, a_1, \ldots)$ de elementos de K,de la que todos los términos a_i a excepción de su número finito son nulos, y se denomina serie seudo -infinita sobre $\mathcal{K}$.Para toda serie seudo-infinita a existe un numero natural n tal que $a_i = 0$ para todo $i \ge n$. El conjunto de todas las series seudo-infinitas sobre $\mathcal{K}$ será denotada L_1.

Introdúzcase sobre el conjunto L_1 la relación de igualdad que plantea $(a_0, a_1, \ldots) = (b_0, b_1, \ldots)$ si y solo si $a_i = b_i$ para todo número natural i.

La suma de dos elementos cuales quiera $a = (a_0, a_1, \ldots)$ y $b = (b_0, b_1, \ldots)$ está definida por la igualdad

$$a \oplus b = (a_0 + b_0, a_1 + b_1, \ldots).$$

Se denotara más adelante que $(a \oplus b)i$ es la $i-ésima$ componente de la suma $a+b$.

El producto del elemento λ de K por el elemento a de L_1 se define por la formula $\lambda_a, \lambda a_1, \ldots)$. En particular, se plantea $\ominus a = (-1)a = (-a_0, -a_1, \ldots)$.

La suma en L_1 es conmutativa, asociativa y dotada de un elemento neutro $0 = (0, 0, \ldots)$; Además, para cada a de L_1 $\ominus a$ es un elemento opuesto, quiere decir que $a \oplus (\ominus a) = 0$. Por tanto, el algebra $\langle L_1, \oplus, \ominus\rangle$ es un grupo conmutativo.

El producto de dos elementos cual quiera $a = (a_0, a_1, \ldots)$ y $b = (b_0, b_1, \ldots)$ de L_1 se define por la formula

$(a_0, a_1, \ldots) \odot (b_0, b_1, \ldots) = c_0, c_1, \ldots),$

donde $c_{\mathcal{R}} = \sum_{i+j=\mathcal{R}} a_i b_i$ para todo numero natural $\mathcal{K}$. Más adelante se denotara por (a $\odot b$)$_{\mathcal{R}}$ la $k-ésima$ componente del producto ab.

Así que, sobre el conjunto L_1 se tiene definido dos operaciones binarias (la suma $\oplus$ y la multiplicación $\odot$) y la operación simple $\ominus$ que asocia a cada $\odot$ de L_1 un elemento opuesto $\ominus a$. De ahora en adelante 1 es la unidad del anillo $\mathcal{K}$, $1 = 1_{\mathcal{K}}$ y $1 = (1,0,0\ldots)$.

LEMA 1.3. Un algebra $L_1 = \langle L_1, \oplus, \ominus, \odot, 1 \rangle$ es un anillo conmutativo.

Demostración. Se tiene establecido anteriormente que el álgebra $\langle L_1, \oplus, \ominus \rangle$ era un grupo abeliano. De la definición de la multiplicación en L_1 se deduce directamente que esta es conmutativa. La multiplicación en L_1 es asociativa. En efecto, para todos a, b, c de L_1

$$\left(a \odot \left(b \bigodot c\right)\right) i = \sum_{j+s=i} a_j (b \cdot c)_s = \sum_{j+s=i} a_j \left(\sum_{k+l=s} b_k c_1\right) =$$

$$= \sum_{j+k+l=i} a_j b_k c_l$$

$$((a \odot b) \odot c)_{i=} \sum_{t+l=i} (ab)_t \, c_{l=} \sum_{t+l=i} \left(\sum_{j+k=t} a_j b_k\right) c_l = \sum_{j+k+l=i} a_j b_k c_l.$$

Por tanto, $a \odot (b \odot c) = (a \odot b) \odot c$.

La multiplicación en L_1 es distributiva con relación a la suma. Efectivamente, para todos a, b, c de L_1

$$((a \oplus b) \odot c)_{i=} \sum_{j+k=i} (a \oplus b)_j \, c_{k=} \sum_{j+k=i} \left(a_j c_k + b_j c_k\right),$$

$$(a \odot c \oplus b \odot c)_{i=} (a \odot c)_i \oplus (b \odot c)_{i=} \sum_{j+k=i} a_j c_k + \sum_{j+k=i} b_j c_k$$

$$= \sum_{j+k=i} \left(a_j c_k + b_j c_k\right).$$

Por tanto, $(a \oplus b) \odot c = a \odot c \oplus b \odot c$. Asi mismo, $\overline{1}$ es un elemento neutro con relación a la multiplicación en L_1.

En resumen, se tiene establecido que el algebra L_1 es un anillo conmutativo. □

Plantéese

$$u_0 = (1,0,0,\ldots), u_1 = (0,1,0,0,\ldots), \ldots, u_k = \underbrace{(0,\ldots,0,1,0}_{k \; ceros}, \ldots).$$

Un elemento cualquiera $a = (a_0, a_1, \ldots)$ de L_1 puede estar escrito bajo la forma

$$a = a_0(1,0,0,\ldots) \oplus a_1(0,1,0,\ldots) \oplus \ldots \oplus a_n(0,\ldots,0,1,0,\ldots) = a_0 u_0 \oplus a_1 u_1 \oplus \ldots \oplus a_n u_n,$$

quiere decir,

$$a = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n,$$

donde n es un número natural tal que $a_i = 0$ para todo $i > n$.

Para todo número natural n el sistema de elementos $u_0, u_1, \ldots, u_n$ es linealmente independiente sobre k, quiere decir que para todos los elementos $\lambda_0, \lambda_1, \ldots, \lambda_n$ del conjunto k de la igualdad

$$(1) \quad \lambda_0u_0 \oplus \lambda_1, u_1 \oplus \ldots \oplus \lambda_nu_n = \bar{0}$$

se deducen las igualdades $\lambda_n = 0,\ \lambda_1 = 0, \ldots, \lambda_n = 0$.

Efectivamente, de (1) se deduce

$\lambda_0u_0 + \lambda_1u_1 + \ldots + \lambda_nu_n(\lambda_0, \lambda_1, \ldots, \lambda_n, 0, 0, \ldots) = (0,0,0, \ldots)$,

por lo tanto $\lambda_0 = 0, \lambda_1 = 0, \ldots, \lambda_n = 0$.

Plantéese que $x = u_1 = (0,\ 1,\ 0,\ 0, \ldots)$. De la definición de la multiplicación en L_1, se deduce que

$x^2 = u_2, x^2 = u_2 \odot u_1 = u_3, \ldots, x^2 = u_{nn-1} \odot u_1 = u_n$.

Por tanto, cada elemento a de L_1 para el cual $a_i = 0$ para todo $i > n$ puede estar representada bajo la forma

$a = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n = a_0u_0 \oplus a_1x \oplus \ldots \oplus a_nx^n$.

TEOREMA 1.4. Para cualquier anillo conmutativo integro $k = \langle K, +, -, ., 1\rangle$ existe una extensión trascendente simple.

Demostración. Sea L_1 un conjunto de todas las series seudo-infinitas sobre k. Según el lema 1.3, el algebra

$$\mathcal{L}_1 = \langle \mathcal{L}_1, \otimes, \ominus, \odot, \bar{\bar{1}} \rangle$$

es un anillo conmutativo. El conjunto

$K_1 = \{a_0u_0 \mid a_0 \in K\}$, Donde $a_0u_0 = \{a_0, 0, 0, \ldots\}$,

es cerrado en el anillo $\mathcal{L}_1$ y es no vacío. Por tanto, el algebra

$$k_1 = \langle K, \oplus, \ominus, \odot, \bar{1} \rangle$$

es un sub-anillo del anillo $\mathcal{L}_1$. La aplicación $h_1 : K_1 \to K$ tal que

$h_1(a_0u_0) = a_0$ Para cada a_0 de K

es aparentemente una función inyectiva del conjunto K_1 sobre K. Ademas, h_1 respeta las operaciones principales del anillo k_1,puesto que para todos $a_0,\ b_0$ de K, se tiene

$h_1(a_0u_0 \oplus b_0u_0) = a_0 + b_0$,
$h_1(\ominus a_0u_o) = -a_0$,
$h_1(a_0u_0 \odot b_0u_0) = a_0 \cdot b_0$,
$h_1(1 \odot u_0) = 1$ (es decir que $h_1(\bar{1}) = 1_k$).

Por tanto, h_1 es un isomorfismo del anillo k_1 sobre k. De este modo, $\mathcal{L}_1$ posee un sub-anillo k_1 isomorfo en el anillo k.

Sobre la base del anillo $\mathcal{L}_1$ se debe construir un nuevo anillo isomorfo a $\mathcal{L}_1$ y que contenga el sub-anillo k.Para ello, substitúyase en el conjunto $\mathcal{L}_1$ el elemento a_0 de k en cada elemento a_0u_0 $de\ k_1$ (dicho de otro modo, substitúyase el elemento $h_1(a_0u_0)$ en a_0u_0) que deja a todos los otros elementos del conjunto $\mathcal{L}_1$ iguales. Plantéese

$L = (\mathcal{L}_1 \setminus K_1) \cup K$

Y defínase la aplicación h: $\mathcal{L}_1 \to L$ de la manera siguiente:

$$h(a) = \begin{cases} h_1(a)\ si\ a \in k_1; \\ a \quad si\ a \in \mathcal{L}_1 \setminus k_1. \end{cases}$$

Se observa fácilmente que h es una aplicación inyectiva del conjunto $\mathcal{L}_1$ sobre L que prolonga la aplicación h_1, quiere decir $h_1 \subset h$.

Defínase sobre conjunto L las operaciones $+, -, \bullet, 1$ por las fórmulas

$a + \beta = h\big(h^1(a) \oplus h^{-1}(\beta)\big)\ (a, \beta \in L)$;

$-a = h\big(\ominus\, h^{-1}(a)\big)$;

(I) $a.\beta = h(h^{-1}(a) \odot h^{-1}(\beta))$;

$1 = h\,(\bar{1}) = 1_k$.

Considérese el algebra $\mathcal{L} = \langle L, +, -, \bullet, 1\rangle$. De las Fórmulas (I) se deducen las fórmulas

$h^{-1}(a + \beta) = h^{-1}(a) \oplus h^{-1}(\beta)$;

$h^{-1}(-a) = \ominus\, h^{-1}(a)$;

(II) $h^{-1}(a \bullet \beta) = h^{-1}(a) \odot\ h^{-1}(\beta)$;

$h^{-1}(1) = \bar{1}$.

Las fórmulas (II) muestran que h^{-1} es un isomorfismos del algebra $\mathcal{L}$ sobre el anillo $\mathcal{L}_1$. Se deduce que el algebra $\mathcal{L}$ es un anillo conmutativo isomorfo en el anillo $\mathcal{L}_1$.Las operaciones principales en el anillo $\mathcal{L}$ constituyen prolongaciones de operaciones correspondientes en el anillo k. En efecto, conforme a (I),para todos a y β de K, se tiene:

$a + \beta = h(h^{-1}(a) \oplus h^{-1}(\beta)) = h(au_0 \oplus \beta u_0) = h(au_0) + h(\beta u_0) = h_1(au_0) + h_1(\beta u_0) = a + \beta$;

$-a = h\big(\ominus\, h^{-1}(a)\big) = h(\ominus\, au_0) = -h(au_0) = -h_1((au_0) = -a$;

$(a \bullet \beta) = h(h^{-1}(a) \odot h^{-1}(\beta)); = h(au_0) \odot \beta u_0) = h(au_0) \bullet h(\beta u_0) = h_1((au_0) \bullet h_1(\beta u_0) = a\,\beta$.

Por tanto, k es un sub-anillo del anillo $\mathcal{L}$.

Todo elemento de $\mathcal{L}$ puede estar representado bajo la forma de una combinación lineal de elementos $1, x, x^1, \ldots$ con coeficientes en K, puesto que

$h(a_0u_0 \oplus \ldots \oplus a_nu_n) = a_0 + a_1u_1 + \ldots a_nu_n = a_0 + a_1x + \cdots + a_nu_n = a_0 + a_1x + \cdots + (a_i \in K)$.

Por tanto, $\mathcal{L} = k[x]$.

El elemento x es trascendente sobre k. De hecho, la igualdad

$a_0 + a_1x + \cdots + a_nh^n = 0$

implica la igualdad

$$h^{-1}(a_0 + a_1x + \cdots + a_nx^n) = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n = \overline{0}.$$

Ya que los elementos $u_0, \ldots, u_n$ son linealmente independientes sobre k_1, se deduce que $a_0 = 0,\ a_1 = 0, \ldots\ , a_n = 0$. Por lo tanto x es un elemento trascendente sobre k y el anillo $\mathcal{L} = k[x]$ es una extensión trascendente del anillo k por adjunción de x. □

Grado de un polinomio. Sean k un anillo conmutativo íntegro y $k[x]$ un anillo de los polinomios en x, quiere decir que es una extensión trascendente simple de k por adjunción de x. Todo elemento no nulo a de $K[x]$ puede estar representado de manera única bajo la forma de una combinación lineal de potencias de x con coeficientes en K.

DEFINICIÓN. Sea a un polinomio de $K[x]$. Se denomina *grado de un polinomio* a al número natural $n\ si\ a = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$. En este caso $a_0,\ a_1, \ldots, a_n$ son los coeficientes del polinomio, el elemento a_n es el coeficiente principal. El polinomio a se denomina mónico si su coeficiente dominante es igual a la unidad del anillo k.

Se notara el grado de un polinomio a gr a.

Así, como el grado de un polinomio se definió para todo polinomio salvo para el polinomio nulo; el grado de un polinomio nulo no se determina. El grado de un polinomio a_0 donde a_0 es un elemento no nulo del anillo k, que vale cero.

Nótese algunas propiedades del grado de un polinomio.

PROPOSICIÓN 1.5. *El grado de una suma de dos polinomios no nulos es como máximo igual al grado máximo de sus términos, quiere decir que el* $gr\ (a + b) \leq max(gr\ a, gr)$.

PROPOSICIÓN 1.6. *El grado de un producto de dos polinomios no nulos es como máximo igual a la suma de los grados de cofactores, quiere decir con* $ab \neq 0\ gr \leq gr\ a + gr\ b$.

La demostración de las Proposiciones 1.5 y 1.6 se deja a la opción del lector.

PROPOSICIÓN 1.7. *Si k es un dominio de integridad, el grado de un producto de dos polinomios no nulos es igual a la suma de los grados de cofactores, quiere decir al* $gr(ab) = gr\ a + gr\ b$.

Demostración. Sean $a = a_0 + \cdots + a_mx^m$, $b = b_0 + \ldots + b_nx^n$ de los polinomios sobre el dominio de integridad siendo k y $a_m \neq 0, b_m \neq 0$. Entonces se tiene $ab = a_0b_0 + (a_0b_1 + a_1b_0)\ x + \ldots + a_mb_nx^{m+n}$. Si k tiene el dominio de integridad, se tiene $a_mb_n \neq 0$.

Por lo tanto, gr $(ab) = m + n =$ gr a + grb. □

TEOREMA 1.8. *Si k es un dominio de integridad, entonces el anillo de los polinomios $K[x]$ es también un dominio de integridad*.

Este TEOREMA se deriva directamente de la proposición 1.7.

De los TEOREMAs 1.8 y 13.2.1. Se deriva el corolario siguiente:

COROLARIO 1.9. *Para un anillo de polinomios $k[x]$sobre el dominio de integridad k existe n un cuerpo de cocientes.*

División de un polinomio por un binomio y raíces de un polinomio. *Sea* $k[x]$ un anillo de polinomios en $K[x]$ en x sobre un anillo conmutativo integro k.Si $f = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ y $c_0 \in K$, entonces la suma de $a_0 + a_1c_0 + \ldots + a_nc_0^n$ será denotada $f(c_0)$ y denominada *valor de un polinomio para el argumento* c_0.

TEOREMA 1.10 (de Bézout). Sean f un polinomio sobre el anillo k y $c_0 \in K$. En el anillo $k\ [x]$ existe un polinomio q tal que $f = (x - c_0)q + f(c_0)$.

Demostración. El TEOREMA es verdadero si f es un polinomio nulo; en ese caso $f(c_0) = 0$ y se puede plantear $q = 0$. Sea $f = a_0 + a_1x^1 + \ldots + a_nx^n$ un polinomio no nulo, entonces se cumple que

$$f - f(c_0) = a_1(x - c_0) + a_2(x^2 - c_0^2) + \ldots + a_n(x^n - c_0^n)$$
$$= (x - c_0)[a_1 + a_2(x + c_0) + \ldots + a_n(x^{n-1}. + c_0x^{n-2} + \ldots + c_0^{n-1})];$$

por tanto, $f = (x - c_0)q + f(c_0)$, donde

$$q = a_1 + a_2(x + c_0) + \ldots + a_n(x^{n-1} + \ldots + c_0^{n-1}) \in K[x] \,.\, \square$$

El TEOREMA de Bézout con frecuencia se enuncia de la manera siguiente: *el resto de la división del polinomio f de $K[x]$, donde k es un anillo conmutativo, por el binomio $(x - c_0), c_0 \in K$, y equivale a $f(c_0)$.*

Sea f un polinomio sobre el anillo $k, c_0 \in K$.

DEFINICIÓN. Al elemento c_0 del anillo k se le denomina *raíz del polinomio f sobre el anillo k* si $f(c_0) = 0$.

TEOREMA 1.11. *Sean f un polinomio sobre el anillo k Y $c_0 \in K$. El elemento c_0 es una raíz de un polinomio f si y solo si $x - c_0$ divide el polinomio f en el anillo $k[x]$.*

Demostración. Sea c_0 una raíz de un polinomio $f, f(c_0) = 0$. Según el TEOREMA de Bézout, $f = (x - c_0)q, \text{donde } q \in K[x]$. Por tanto, $x - c_0$ divide al polinomio f en $k[x]$.

Ahora supóngase que $x - c_0$ divide el polinomio f en el anillo $k[x]$, quiere decir que $f = (x - c_0)\text{g}, \text{ donde g} \in K[x]$. Por lo tanto, $f(c_0) = (c_0 - c_0)\,\text{g}\,(c_0) = 0$. $\square$

TEOREMA concerniente al número máximo posible de las raíces de un polinomio en un dominio de integridad. Sea $k[x]$ un anillo de polinomios sobre el anillo k.

TEOREMA 1.12. *Sea k un dominio de integridad. Todo polinomio de $K[x]$ de grado n posee en k n raíces diferentes como máximo*.

La demostración está dirigida por inducción sobre n.

Si gr $f = 0$, quiere decir que si $f = a_0, \text{donde } a_0 \in K$ y $a_0 \neq 0$, por lo tanto el polinomio f no tiene raíces. Supóngase que un polinomio cualquiera de $K[x]$ de grado n posee n raíces como máximo. Sean $f \in K[x]$ y gr $f = n + 1$. Si f no tiene raíces en k,entonces el TEOREMA es verdadero. Si, en cambio, f tiene raíces en k, entonces $f(c_0) = 0$. Para un cierto elemento c_0 de K. Según el TEOREMA de Bézout, $f = (x - c_0)\text{g}, \text{ donde g} \in K[x]$; además, ya que k es un dominio de integridad, en virtud de la proposición 1.7, el grado de un polinomio g equivale a n. El elemento b_0 del anillo k,diferente de c_0, es una raíz del polinomio f si y solo si $f(b_0) = (b_0 - c_0)\,\text{g}(b_0) = 0$, quiere decir que si $\text{g}(b_0) = 0$,dado que k es un dominio de integridad. El grado de g es n,por hipótesis de Inducción, g tiene como máximo n raíces diferentes en k. Por lo tanto, el polinomio f de grado $n + 1$ como máximo posee en k $n + 1$ raíces diferentes. $\square$

COROLARIO 1.13. *Si el polinomio $f = a_0 + \ldots + a_nx^n \in K[x]$ posee por lo menos en el dominio de integridad k n raíces diferentes, por lo tanto f es un polinomio nulo*.

Igualdades algebraicas y funcionales de polinomios. Sean $K[x]$ un anillo de polinomios sobre un dominio de integridad K y $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]$. Notese f^* la aplicación

$$\{\langle \lambda, a_0 + a_1\lambda + \ldots + a_n\lambda^n \rangle \mid \lambda \in K\}$$

que asocia a cada λ de K el elemento $f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n$, quiere decir el valor del polinomio f para el argumento λ. Para ciertos anillos de k de polinomios diferentes pueden definir la misma función. Es asi como por ejemplo, si $z_2 = z/2\,z$ y $z_2[x]$ es un anillo de polinomio sobre el cuerpo z_2, los polinomios $x + x^2$, $x - x^2$ y 0 definen entonces la misma función.

TEOREMA 1.14. Sea $k[x]$ un anillo de polinomios sobre un dominio de integridad infinito K. Los polinomios f y g de $K[x]$ son iguales si y solo si son iguales las funciones f y g de los polinomios de $K[x]$ y f^* y g^* que estos definen.

Demostración. Sean f y g polinomios de $K[x]$ y f^*, g^* las funciones que estos definen.
Supóngase que $f = \mathrm{g}$. Si f y g son polinomios nulos, por lo tanto $f^* = \mathrm{g}^*$. Supóngase que f y g son polinomios no nulos de grado n:

$$f = a_0 + a_1x + \ldots + a_nx^n, \quad \mathrm{g}(x) = b_0 + b_1x + \ldots + b_nx^n.$$

Como $f = \mathrm{g}$, se tiene

(1) $a_0 + b_0, \ldots, a_n = b_n$.

Para todo $\lambda\ de\ K$, se cumple:

$$f^*(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n, \quad \mathrm{g}^*(\lambda) = b_0 + b_1\lambda + \ldots + b_n\lambda^n .$$

Por lo tanto, conforme a (1), $f^* = \mathrm{g}^*$.
Plantéese ahora que $f^* = \mathrm{g}^*$, quiere decir que para todo λ de K, se tiene

$f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n = \mathrm{g}(\lambda) = b_0 + b_1\lambda + \ldots + b_n$
En este caso, para todo polinomio $h = f - \mathrm{g}$, este satisface la condición

(2) $h(\lambda) = 0$ para todo f de K.
El conjunto K que es infinito, (2) significa que el polinomio h posee una infinidad de raíces diferentes. Según el *corolario 1.13*, h es un polinomio nulo, quiere decir que
$f - \mathrm{g} = 0$ y $f = \mathrm{g}$. Es asi como, se deducen de $f^* = \mathrm{g}^*$ que $f = \mathrm{g}$. □

Ejercicios

1. Demostrar las proposiciones 1.5 y 1.6
2. Sea $\mathcal{F}[x]$un anillo de polinomios en el cuerpo $\mathcal{F}$ y I un conjunto no vacío de $F[x]$ cerrado conforme a la sustracción y que satisface a las condiciones: si $f \in I$, entonces $x.f \in I$ y $\lambda f \in I$ para todo λ de F. Demostrar que el conjunto I es un ideal del anillo$\mathcal{F}[x]$.
3. Buscar todos los automorfismos del anillo de los polinomios $Z[x]$.
4. Buscar todos los automorfismos del anillo de los polinomios $Q[x]$.
5. Buscar todos los automorfismos del anillo de los polinomios $R[x]$.
6. Buscar todos los automorfismos del anillo de los polinomios $\mathcal{C}[x]$ en el cuerpo $\mathcal{C}$ de los números complejos.
7. Sea $\mathcal{Z}[x]$ un anillo de polinomios en el anillo $\mathcal{Z}$ de enteros. Demuéstrese que el conjunto de todos los polinomios de $Z[x]$ en términos libres pares es un ideal del anillo $\mathcal{Z}[x]$ aunque no sea un ideal principal.

§ 2. Polinomios en un cuerpo.

TEOREMA de la división con resta. Sea $\mathcal{F}[x]$ un anillo de polinomios en el cuerpo $\mathcal{F}$ y $F[x]$ su conjunto de base.

TEOREMA 2.1. Sea *hun polinomio no nulo de* $F[x]$. *Para cada polinomio* f *de* $F[x]$*existe en* $F[x]$ *una pareja única de polinomios* q *y* r *tales que*

(1) $f = \mathrm{h}.\mathrm{q} + \mathrm{rygrad\ r} < \mathrm{grad}\, h$ o $\mathrm{r} = 0$.

Demostración. Comiéncese por demostrar por deducción en el grado$n$ del polinomio f ya que existen polinomios q y $r$que satisfacen las condiciones (1). Sea

$$\operatorname{grad} h = m, \qquad h = b_0 + \ldots + b_m x^m (b_m \neq 0).$$

Nótese que si f es un polinomo nulo en $\operatorname{grad} f < m$, entonces $f = h.0 + f$ y, por consiguiente, puede notarse $q = 0$ y $\mathrm{r} = f$.Por lo tanto nos quedas estudiar el caso donde $\operatorname{grad} f \geq m$. Supóngase que el TEOREMA es verdadero para cualquier polinomio$f$ de grado inferior an. Sea $\operatorname{grad} f = n \geq m$. En este caso los polinomios f y $a_n b_m^{-1} x^{n-m} h$ poseen los mismos coeficientes dominantes. Por tanto, el polinomio

(2) $g = f - a_n b_m^{-1} x^{n-m}.h$

es bien polinomio de grado cero, o bien su grado es inferior a n si $\mathrm{g} = 0$, entonces $f = a_n b_m^{-1} x^{n-m} h + 0$ y se puede plantear $q = a_n b_m^{-1} x^{n-m}$ y $\mathrm{r} = 0$. Si, por el contrario, $\operatorname{grad} \mathrm{g} < n$, entonces, por hipótesis de deducción, existe en $F[x]$ polinomios q y r tales que

(3) $\mathrm{g} = h\bar{q} + r$ y $\operatorname{grad} r < grad\ h$o $r = 0$.

Conforme a (2) y (3), $f = h(\bar{q} + a_n b_m^{-1} x^{n-m}) + r$ o si se plantea $q = \bar{q} + a_n b_m^{-1} x^{n-m}$

(4) $f = h.q + r$ y $r = 0$ o $\operatorname{grad} r < \operatorname{grad} h.$

Demuéstrese que para los polinomios fy h dados el “cociente incompleto”q y la “residuo” r en (4) se define de manera univoca. De hecho, supóngase que

(5) $f = hq_1 + r_1$ y $r_1 = 0$ o $\operatorname{grad} r_1 < \operatorname{grad} h \quad (r_1, q_1 \in F[x]).$

Entonces, conforme a (4) y (5), se obtiene.

(6) $r_1 - r = h(q - q_1), \qquad r_1 - r = 0$ o $\operatorname{grad}(r_1 - r) < \operatorname{grad} h.$

Si $r_1 - r \neq 0$, entonces $q - q_1 \neq 0$ y

$$\operatorname{grad}(r_1 - r) = \operatorname{grad} h + \operatorname{grad}(q - q_1) \geq \operatorname{grad} h,$$

lo que es una contradicción con las condiciones (6). Pero si $r_1 - r = 0$, entonces $q - q_1 = 0$ y por consiguiente, $q = q_1$. □

COROLARIO 2.2 *Si $\mathcal{F}$ es un cuerpo, el anillo de los polinomios $\mathcal{F}[x]$ es entonces un anillo euclidiano.*

COROLARIO 2.3. *Un anillo de polinomios $\mathcal{F}[x]$ en el cuerpo $\mathcal{F}$es un anillo de ideales principales.*

COROLARIO 2.4. S*i $\mathcal{F}$ es un cuerpo, el anillo de polinomios $\mathcal{F}[x]$ es entonces un anillo factorial.*

Algoritmo de Euclide. Sea $\mathcal{K}$ un anillo conmutativo.

LEMA 2.5. *Supóngase que se obtiene en un anillo conmutativo $\mathcal{K}$ para los elementos a, b, q y r la igualdad.*

(1) $a = bq + r$;

Entonces

(2) $MCD(a, b) \sim MCD(b, r)$.

Demostración. Sea $d = MCD(a,b)$, $d' = MCD(b,r)$.dado que $d|a, d|b$, entonces conforme de (1), $d|r$. d sea el divisor común de b y r, se tiene $d|d'$. De manera análoga se demuestra que $d'|d$. por tanto, $d \sim d'$. □

Para encontrar el MCD de dos elementos del anillo de los polinomios $\mathcal{F}[x]$ (o todo anillo euclidiano) se utiliza el procedimiento "de divisiones sucesivas" llamado *algoritmo de Euclide.* Este proceso consiste en calcular MCD de los polinomios obtenidos de a, b de $F[x]$ que busca el MCD de los polinomios b y r en grados inferiores.

Supóngase que ninguno de los polinomios a, b se dividen (en $\mathcal{F}[x]$) por el otro y supóngase $b = b_1$; entonces

$$a = b_1 q_1 + b_2; \operatorname{grad} b_1 > \operatorname{grad} b_2,$$

$$b_1 = b_2 q_2 + b_3, \qquad \operatorname{grad} b_2 > \operatorname{grad} b_3.$$

Esta operación continúa hasta que sólo se obtenga un cero después de una división:

$$b_{R-2} = b_{R-1} q_{R-1} + b_R, \quad \operatorname{grad} b_{R-1} > \operatorname{grad} b_R,$$

$$b_{R-1} = b_R q_R + 0.$$

Nótese que la sucesión $\operatorname{grad} b_1, .\operatorname{grad} b_2$, . . . es una sucesión de creciente de números naturales. Esta es la razón de su conclusión después de un número no finito. Supóngase que $b_R \neq 0$ y $b_{R+1} = 0$; entonces

$$\operatorname{grad} b_1 > \operatorname{grad} b_2 > \operatorname{grad} b_3 > . \; . \; . > \operatorname{grad} b_{R-1} > \operatorname{grad} b_R.$$

En la base del lema 2.5, de las igualdades antes mencionadas se deduce.

$$MCD(a_1, b_1) \sim MCD(b_1, b_2) \sim . \; . \; . \sim MCD(b_{R-1}, b_R) \sim$$

$$\sim MCD(b_R, 0) = b_R.$$

Así, $MCD(a,b) \sim b_R$ y $b_R$es $MCD(a,b)$.

Se llega a la siguiente conclusión. *Si en los polinomios del anillo $\mathcal{F}[x]$ se aplica el algoritmo de Euclide, entonces se obtiene de la última resta no nula elMCDde los polinomios a y b.*

COROLARIO 2.6. *Sean$\mathcal{F}$ un sub- cuerpo del cuerpo $\mathcal{P}$,$\mathcal{F}[x]$ y $\mathcal{P}[x]$ de los anillos de los polinomios respectivamente en $\mathcal{F}$ y en $\mathcal{P}$.*

Sea a y b polinomios no simultáneamente nulos de $\mathcal{F}[x]$ .Si d y d'son los máximos común divisor extraídos de los polinomios a y b respectivamente en $\mathcal{F}[x]$ y $\mathcal{P}[x]$, entonces se tiene $d = d'$.

Polinomios irreducibles en un cuerpo dado. Sea $\mathcal{F}[x]$ un anillo de polinomios sobre el cuerpo$\mathcal{F}$. En el anillo $\mathcal{F}[x]$son recíprocos solamente los polinomios de grado cero (divisores unitarios del cuerpo $\mathcal{F}$,) es decir los elementos no nulos del cuerpo$\mathcal{F}$. Por lo tanto, cualquier polinomio de grado positivo de $\mathcal{F}[x]$ es irreversible en el anillo $\mathcal{F}[x]$.

Un polinomio de $\mathcal{F}[x]$ es *reducible* o *compuesto* en el anillo $\mathcal{F}[x]$ o reducible en el cuerpo $\mathcal{F}$si se puede representar bajo la forma de producto de dos polinomios de grado positivo de $\mathcal{F}[x]$.

En otras palabras, un polinomio es reducible en $\mathcal{F}[x]$ si tiene un grado positivo y posee divisores no triviales.

Un polinomio de $\mathcal{F}[x]$*es irreducible o primo* en el anillo $\mathcal{F}[x]$ o irreducible en el cuerpo $\mathcal{F}$ si tiene un grado positivo y no solamente posee divisores triviales, es decir que cualquier divisor del polinomio se asocia ya sea este último, o sea en la unidad.

También, el polinomio a es irreductible en el anillo $\mathfrak{F}[x]$ si es de grado positivo e en toda descomposición de la forma $a = bc$, o $b, c \in \mathcal{F}[x]$, uno de los factores (b o c) asociado a la unidad del cuerpo, y otro en a.

Ejemplos: 1. Si $\mathfrak{F}$ es un cuerpo, entonces en el anillo de los polinomios $\mathfrak{F}[x]$ todo polinomio de primer grado es irreductible.

2. En un anillo de polinomios $\mathcal{R}[x]$, donde $\mathcal{R}$ es un cuerpo de números reales, el polinomio de segundo grado es irreductible si y sólo si no admite raíces reales.

PROPOSICIÓN 2.7. *Sea p un polinomio irreductible y a todo polinomio del anillo $\mathcal{F}[x]$, entonces, sea p divise a, es decir p y a primos entre estos.*

Demostración. Se supone que$\mathcal{F}$ es un cuerpo. Según el corolario 2.3, $\mathcal{F}[x]$ es un anillo de ideas principales. Por lo tanto, conforme a 13.3.9, si p no divide$a$, se tiene entonces $(p, a) = (1)$. Así pues tenemos $\lambda_{1p} + \lambda_{2a} = 1$ para algunos λ_1, λ_2 de F. Por consiguiente según el TEOREMA 13.4.4, el máximo común divisor de p y a es 1, es decir los polinomios p y a son primos entre ellos. □

PROPOSICIÓN 2.8. *Sea $p$un polinomio irreducible en el anillo $\mathcal{F}[x]$ y $a_1, \ldots, a_n \epsilon F[x]$.si p divide el producto $a_1, \ldots, a_n$.Entoncespdivide al menos uno de los polinomios $a_1, \ldots, a_n$.*

Esta proposición se deriva directamente del corolario 2.3 y de la proposición 13.3.11.

TEOREMA 2.9. *Sea $\mathcal{R}[x]$un anillo de polinomios en el cuerpo $[\mathcal{R}]$ de números reales. El anillo cociente $\mathcal{R}[x]/(x^2 + 1)$ es isomorfo al cuerpo de números complejos.*

Demostración. Sea C el conjunto de base del cuerpo $\mathcal{C}$ de números complejos. Sea h la función del conjunto $\mathbf{R}[x]$ en $\mathcal{C}$ tal que

$h(f) = f(i)$ Para todo f de $\mathbf{R}[x]$.

Una verificación directa muestra que h es un epimorfismo del anillo $\mathcal{R}[x]$en el cuerpo $\mathcal{C}$ de números complejos de núcleo $(x^2 + 1)$, es decir $\ker h = (x^2 + 1)$. Por tanto según el TEOREMA 13.1.6. En el epimorfismo de anillo, se obtiene $\mathcal{R}[x]/(x^2 + 1) \cong \mathcal{C}$.□

TEOREMA 2.10. *Sea $\mathcal{F}[x]$ un anillo de polinomios en el cuerpo $\mathfrak{F}$ y p un polinomio irreducible en $\mathfrak{F}[x]$. Entonces el anillo cociente $\mathcal{F}[x]/(p)$ es un cuerpo.*

La demostración de este TEOREMA se deja en manos del lector.

Descomposición de un polinomio en producto de factores normados irreducibles (primos). Sea $\mathcal{F}$ un cuerpo, mientras que $\mathfrak{F}[x]$ es un anillo de polinomio en $\mathfrak{F}$.

TEOREMA 2.11. *Cualquier polinomio de grado positivo de $F[x]$ puede representarse de manera única en forma del producto de un elemento del cuerpo $\mathfrak{F}$ y de polinomios normados irreducibles en $\mathfrak{F}[x]$.*

Demostración. Sea a un polinomio de grado positivo de $F[x]$. Siendo el anillo $\mathfrak{F}[x]$el anillo factorial, el polinomio a puede representarse en forma de producto $a = q_1 \ldots q_s$ de polinomio $q_1, \ldots, q_s$ irreducible en el anillo $\mathfrak{F}[x]$. Sea u_R el coeficiente dominante del polinomio $q_R, u_R \in F$. entonces $q_R = u_R p_R$. donde p_R es un polinomio irreducible en $\mathfrak{F}[x]$.Por lo tanto,

(1) $a = up_1 \ldots p_s$, donde $u = u_1 \ldots u_s \in F$.

Demuéstrese la unicidad de la descomposición. Sea

(2) $a = vp^*_1 \ldots p^*_s, \qquad v \in F,$

una descomposición cualquiera en la cual $p^*_1 \ldots p^*_s$ son polinomios normados irreducibles en el anillo $\mathcal{F}[x]$. Siendo $\mathfrak{F}[x]$ el anillo factorial, se tiene: 1) $u = v$, ya que u, v son coeficientes dominantes de un mismo polinomio a; 2) con una numeración adecuada los polinomios p_i y p_i^* se asocian. Dado que p_i, p_i^* son polinomios normados por el hecho, de estar asociados, resulta $p_i = p_i^*$ para $i = 1, \ldots, s$. □

Sea $a \in F[x]$ y

(1) $a = up_i \ldots p_s$, donde $u \in F$,

es una descomposición del polinomio a en un producto de factores normados irreducibles en $\mathcal{F}[x]$. Sean $p_1, \ldots, p_R$ los diversos factores de normados irreducibles del polinomio a y $\alpha_1, \ldots, \alpha_R$ las multiplicidades de su inmersión en la descomposición (1). Se obtiene entonces la descomposición

(1) $a = up_1\alpha_1 \ldots p_R\alpha_R (u \in F)$.

DEFINICIÓN. *La descomposición* (I)*se le denomina descomposición canónica del polinomio* a *de* $\mathfrak{F}[x]$ *en factores (normados) irreducibles en* $\mathfrak{F}$.

Ejercicios

1. Indicar para cual valor de λ los polinomios $x^3 - 2\lambda x + \lambda^3$ y$x^3 + \lambda^2 - 2$se admite una raíz común en el cuerpo de los números complejos.
2. Buscar el máximo común divisor de los polinomios $x^3 - 1$ y $x^4 + x^3 + 2x^2 + x + 1$ y su representación lineal en función de estos polinomios.
3. Buscar el máximo común divisor y el mínimo común múltiplo de los polinomios $x^4 - 4x^3 + 1$ y $x^3 - 3x^2 + 1$.
4. Buscar el mínimo común múltiplo de los polinomios $x^{33} - 1$ y $x^{18} - 1$.
5. Sea $\mathfrak{F}[x]$ un anillo de polinomios en el cuerpo $\mathcal{F}$ y a, b, cde los polinomios $F[x]$. Buscar en $F[x]$ el minino ideal que contiene cualquier de estos polinomios.
6. Sea $\mathfrak{F}[x]$ un anillo de polinomio en el cuerpo $\mathfrak{F}$. Demostrar que el conjunto de todos los múltiplos comunes de dos polinomios dados$f$ y g de $F[x]$ es un ideal del anillo $\mathfrak{F}[x]$.
7. Sea x_0 y y_0 polinomios de $F[x]$ que satisfacen a la igualdad $ax_0 + by_0 = c$, donde $a, b, c \in F[x]$. Buscar en $F[x]$ el conjunto de todas las soluciones de la ecuación $ax + by = c$.
8. Demostrar que si el polinomio h es primo con los polinomios f y g, h es primo con $f \cdot g$.
9. Demostrar que el polinomio $x^4 - 2x + 3$ es irreducible en el cuerpo Q.
10. Sea p un polinomio de $F[x]$ tal que cualquier otro polinomio de $F[x]$ siendo este primo de p, o es divisible por p. Demostrar que el polinomio p es irreducible en el cuerpo $\mathfrak{F}$.
11. Sea $\mathfrak{F}[x]$ un anillo de los polinomios en el cuerpo numérico $\mathfrak{F}$. Sea c el grado del polinomio irreducible en $\mathfrak{F}, a, b \in F[x]$ y c divideab. Demostrar que c divide$a$ ob^Rpara un cierto k natural.
12. Sea $f = p_1^{n1}p_2^{n1} \ldots p_k^{nk}$ una descomposición canoníca del polinomio f en el cuerpo $\mathfrak{F}$ ¿cuántos divisores normados en coeficientes en F tiene el polinomio f?
13. Sea $\mathfrak{F}[x]$ un anillo de polinomios en el cuerpo numérico $\mathfrak{F}, p$ un polinomio irreducible$\mathfrak{F}$ y I el ideal generado por el polinomio p. Demostrar que el anillo cociente $\mathfrak{F}[x]/I$ es un cuerpo.

§ 3. Anillo de polinomio factorial en un anillo factorial.

Polinomios primitivos. Más adelante se utilizan las siguientes indicaciones: $\mathcal{K}$ designa un anillo factorial, $\mathfrak{F}$ un cuerpo de cocientes del anillo $\mathcal{K}$; $\mathcal{K}[x]$ un anillo de polinomios en x sobre$\mathcal{K}$; $\mathfrak{F}[x]$un anillo de los polinomios en $x$sobre $\mathfrak{F}$.

DEFINICIÓN. Sea $f = a_0 + a_1x + \ldots + a_nx^n$ un polinomio no nulo cualquiera de $K[x]$. MCD de los coeficientes $a_0, a_1, \ldots, a_n$ en el anillo $\mathcal{K}$llamado *contenido del polinomio* f.

DEFINICIÓN. Un polinomio $f$cuyo contenido es la unidad o el divisor unitario (en $\mathcal{K}$)se denomina *polinomio primitivo en el anillo*$\mathcal{K}[x]$.

El contenido del polinomio f en $\mathcal{K}[x]$ se define de manera unívoca a los factores próximos que son divisores unitarios. En otros términos, dos contenidos cualesquiera del polinomio f se asocian en $\mathcal{K}$.

PROPOSICIÓN 3.1. *Si d es el contenido de un polinomio no nulo de $K[x]$, entonces $f = dg$, donde g es un polinomio primitivo en $\mathcal{K}[x]$.*

Demostración. De hecho, si en el segundo miembro de la igualdad $f = a_0 + a_1x + \ldots + a_nx_n$ anteponiendo d a los paréntesis, se obtiene la igualdad $f = d\left(\frac{a_0}{d} + \frac{a_1}{d}x + \ldots \frac{a_n}{d}x^n\right) = dg$, donde conforme a la preposición 13.4.6, la unidad es el máximo común divisor de los coeficientes $\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_n}{d}$ del polinomio g. Por tanto, g es el polinomio primitivo en $\mathcal{K}[x]$. □

Nótese que todo polinomio de grado positivo irreducible en el anillo $\mathcal{K}$ es primitivo en $\mathcal{K}[x]$. De hecho, si f no es un polinomio primitivo, entonces, según la proposición 3.1, $f = dg$, donde g es el polinomio primitivo en $\mathcal{K}[x]$de grado positivo, mientras que d es el contenido de f. Siendo f no primitivo, d y g son los elementos irreversibles de $\mathcal{K}[x]$. Por tanto, f es reducible en $\mathcal{K}[x]$. Al igual todo polinomio no primitivo de grado positivo es reducible en $\mathcal{K}[x]$ y, por lo tanto todo polinomio de grado positivo irreducible en $\mathcal{K}[x]$ es un polinomio primitivo en $\mathcal{K}[x]$.

Remárquese igualmente que un polinomio primitivo en $\mathcal{K}[x]$ es reducible en $\mathcal{K}$ si y sólo si se puede representar en forma de producto de polinomio de grado positivo (y además primitivos). Para un polinomio no primitivo f cualquiera que no sea verdadero, puesto que $f = dg$, donde d es el contenido de f y $\operatorname{grad} d = 0$, mientras que g es un polinomio primitivo irreducible.

LEMA 3.2. *Sea f, h polinomios primitivos en $\mathcal{K}[x]$ y*

(1) $cf = dh$, donde $c, d \in K\backslash\{0\}$.

Entonces, d se asocia ac en $\mathcal{K}$ y f se asocia ah en $\mathcal{K}[x]$.

Demostración. Sea

$$f = a_0 + \ldots + a_nx^n, \quad h = b_0 + \ldots + b_mx^m$$

$$(a_n \neq 0, b_m \neq 0);$$

entonces, $cf = ca_0 + \ldots + ca_nx^n, dh = db_0 + \ldots + db_mx^m$, conforme a

(1) $n = m$ y

(2) $ca_0 = db_0, \ldots, ca_n = db_n$

Dado que 1 es el máximo común divisor de los coeficientes $a_0, \ldots, a_n$ conforme a la preposición 13.4.5, c es el máximo común divisor de los coeficientes $ca_0, \ldots a_{n,}$. De manera análoga, se sostiene el hecho que h es primitivo y las igualdades (2). Se concluye que d es el máximo común divisor de los coeficientes $ca_0, \ldots, ca_n$. Por tanto$c$ y d se asocian en $\mathcal{K}$ y por consiguiente $d = \varepsilon c$, donde ε es un elemento recíproco del anillo $\mathcal{K}$. dividiéndose los dos miembros de la igualdad (1) por c, se obtiene $f = \varepsilon h$, es decir j y h se asocian en $\mathcal{K}[x]$. □

LEMA 3.3. *Sea f y h los polinomios primitivos en $\mathcal{K}[x]$. Si los polinomios f y h se asocian en $\mathcal{F}[x]$ están igualmente asociados en $\mathcal{K}[x]$.*

Demostración. *Sean f* y h polinomios asociados en $\mathcal{F}[x]$. Se tiene entonces $f = \alpha h$, donde α es un elemento no nulo del cuerpo $\mathcal{F}$. Siendo $\mathcal{F}$un cuerpo de los cocientes del anillo $\mathcal{K}$, el elemento α se puede representar bajo la forma $\alpha = dc^{-1}$, donde $d, c, \in k\backslash\{0\}$.

Así, $f = dc^{-1}h$ y $cf = dh$. Según el lema 3.2, se deduce que los polinomios f yg se asocian en el anillo $\mathcal{K}[x]$.□

LEMA 3.4 (DE GAUSS). *Un producto de los polinomios primitivos en $\mathcal{K}[x]$ es un polinomio primitivo en $\mathcal{K}[x]$.*

Demostración. Sea f y g los polinomios primitivos cualesquiera en $\mathcal{K}[x]$:

$$f = a_0 + a_1x + \ldots + a_mx^m (a_m \in K\backslash\{0\}),$$

$$g = b_0 + b_1x + \ldots + b_nx^n (b_n \in K\backslash\{0\});$$

en este caso,

$$fg = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}\ (c_m + n = a_m b_n \neq 0).$$

Muéstrese que el polinomio fg es primitivo en el anillo $\mathcal{K}[x]$.

Supóngase que p es un elemento primo cualquiera del anillo $\mathcal{K}$ y demuéstrese que al menos los coeficientes del polinomio fg no se divide por p. En efecto conforme al hecho que el polinomio f es primitivo, existe un coeficiente a_r no divisible por p y que posee el menor índice. De manera análoga, existe un coeficiente b_s del polinomio g, no divisible por$p$ y afecta el menor índice.

El coeficiente c_{r+s} del polinomio fgpuede representarse bajo la forma de una suma:

(1) $c_{r+s} = a_r b_s + (a_{r+1}b_{s-1} + \ldots + a_{r-1}b_{s+1} + \ldots\ldots)$.

El primer término de esta suma no es divisible por p, Cuando el segundo, se divide por po falta. Por tanto, el contenido del polinomio fg es 1, es decir, que el polinomio fg es un polinomio primitivo en $\mathcal{K}[x]$. □

LEMA 3.5. *Sea f un polinomio en $\mathcal{K}[x]$.* Si el polinomio *$f$es reducible en $\mathcal{F}[x]$, es igualmente reducible en $\mathcal{K}[x]$.*

Demostración. Sea un polinomio $f$reducible en $\mathcal{F}[x]$, es decir,

(1) $f = gh$,

donde g y h son polinomios de grados positivos de $F[x]$. Admítase que f es irreducible en $\mathcal{K}[x]$ y por consiguiente, primitivo en $\mathcal{K}[x]$.

Sea

$g = \alpha_0 + \alpha_1x + \ldots + \alpha_nx^n$.

Ya que $\mathcal{F}$ es un cuerpo de los cocientes del anillo $\mathcal{K}$, cada coeficiente a_i puede representarse de la forma

$\alpha_i = \alpha_i . b_i^{-1}$, Donde $a_i, b_i \in K$, $\quad (i = 0, \ldots, n)$.

Supóngase $b = b_0 . b_1 \ldots . b_n$; entonces $bg \in K[x]$ y conforme a la proposición 3.1,

(2) $bg = cg_1 (b, c \in K\backslash\{0\})$,

donde g_1 es un polinomio de grado positivo primitivo en $\mathcal{K}[x]$, mientras que c es el contenido del polinomio bg. Se comprueba de la manera análoga que existen elementos d y e tales que

(3) $dh = eh_1 \qquad (d, e \in K\backslash\{0\})$

donde h_1 es un polinomio de grado positivo primitivo en $\mathcal{K}[x]$.

Conforme a (1) (2) y (3), se obtiene

(4) $(bd)f = (ce)g_1h_1 (bd, ce \in K\backslash\{0\})$

además, siguiendo el lema de GAUSS, el polinomio $g_1 h_1$ es primitivo en $\mathcal{K}[x]$, según el lema 3.2 de (4) se deduce que los polinomios f y $g_1 h_1$ se asocian en $\mathcal{K}[x]$. Por tanto

$$f = \varepsilon g_1 h_1,$$

donde ε es un elemento reciproco en K y g_1, h_1 de los polinomios de grados positivos de $K[x]$, que se contradice con la hipótesis admitida.

Así, el polinomio f es reducible en $\mathcal{K}[x]$. □

COROLARIO 3.6. *Si un polinomio de grado positivo es irreducible en el anillo $\mathcal{K}[x]$, es entonces irreducible en el anillo $\mathcal{F}[x]$.*

Anillo factorial de los polinomios. Demuéstrese el TEOREMA principal del siguiente párrafo.

TEOREMA 3.7. *Si el anillo $\mathcal{K}$ es factorial, el anillo de polinomios $\mathcal{K}[x]$ es igual.*

Demostración. Sea $\mathcal{K}$ un anillo factorial. Demuéstrese que todo elemento diferente de cero e irreversible del anillo $\mathcal{K}[x]$se descompone de manera única en un producto de factores primos en $\mathcal{K}[x]$ en orden de cofactores y de factores reciproco próximos. Demuéstrese de acuerdo a las posibilidades de factorización de este elemento. Sea f un polinomio cualquiera no nulo de $K[x]$. Si f es un polinomio de grado cero, entonces $f \in K$. siendo el anillo $\mathcal{K}$ factorial, el polinomio f puede representarse en forma de un producto de factores primos en $\mathcal{K}$ y por consiguiente en $\mathcal{K}[x]$. Supóngase que $\operatorname{grad} f = n > 0$, a continuación se procede a la descomposición de factores primos de cualquier polinomio cuyo grado es inferior en n. Sea

(1) $f = dg(x)$.

donde $d \in K, g(x)$ es un polinomio de grado positivo primitivo en $\mathcal{K}[x]$. Si el polinomio g es irreducible en $\mathcal{K}$, entonces descomponiéndose en (1) el factor d en factores primos, se obtiene una factorización de f. Pero si el polinomio $g(x)$ es reducible en $\mathcal{K}[x]$, puede representarse en forma del producto de dos polinomios de grado positivo e inferior an: $g(x) = h(x)\varphi(x)$. Siguiendo la hipótesis de deducción$h(x)$ y $\varphi(x)$ puede representarseen forma de un producto de factores primos en $\mathcal{K}[x]$. Por tanto g y conforme a (1), f puede igualmente representarse en forma de producto de factores primos.

Demuéstrese la unicidad de la factorización. Sean dados en $\mathcal{K}[x]$ dos factorizaciones de f:

(2) $f = p_1 . \ . \ . \ . p_k q_1 . \ . \ . \ . q_s = p_1' . \ . \ . \ . p' q_1' . \ . \ . \ . q_t'$,

donde $p_i p_i' \in K$ y $q_i q_i'$ son polinomios de grados positivos irreducibles y por lo tanto, primitivos. Según los lemas 3.2 y 3.4. Se deduce de (2)

(3) $p_1 . \ . \ . \ . p_k \sim p_1' . \ . \ . \ . p_r'$ en $\mathcal{K}$;

(4) $q_1 . \ . \ . \ q_s \sim q_1' . \ . \ . \ q_t'$ en $\mathcal{K}[x]$.

Siendo el anillo $\mathcal{K}$ factorial, se deduce de (3) que $k = r$ y para una numeración adecuada

(5) $p_i \sim p_i'$ en $\mathcal{K}, i = 1, . \ . \ . \ , k.$

Además, según el corolario 3.6, los polinomios q_i y q_i' son irreducibles en el anillo $\mathcal{F}[x]$. Conforme al hecho que el anillo $\mathcal{F}[x]$ es factorial, se deduce de (4) que $s = t$ y para una numeración apropiada

$q_i \sim q_i'$ En $\mathcal{F}[x], . i = 1, . \ . \ . \ , s.$

Los polinomios q_i y q_i' son irreducibles en $\mathcal{K}[x]$ y por consiguiente primitivos en $\mathcal{K}[x]$ por otra parte, estos polinomios se asocian en $\mathcal{F}[x]$. Por tanto, según el lema 3.3, estos se asocian en $\mathcal{K}[x]$:

(6) $q_i \sim q_i'$ En $\mathcal{K}[x], . i = 1, . \ . \ . \ ., s.$

Conforme a (5) y (6), el polinomio f presenta una factorización única en factores primos en el anillo $\mathcal{K}[x]$. En breve se demuestra que el anillo $\mathcal{K}[x]$ es factorial. □

Ejercicios

1. ¿El polinomio $x^2 + 2x + 2$ es reducible o irreducible: (a) en el anillo $\mathcal{Q}[x]$; (b) en el anillo $\mathcal{R}[x]$; (c) en el anillo $\mathcal{C}[x]$?
2. ¿El polinomio $2x + 6$ es reducible o irreducible: (a) en el anillo $\mathcal{Q}[x]$; (b) en el anillo $\mathcal{Z}[x]$?
3. Cualquier polinomio irreducible en el anillo $\mathcal{Z}[x]$ es un polinomio primitivo en $\mathcal{Z}[x]$. ¿Es que la reciprocidad es verdadera?

§ 4. Derivada formal de un polinomio. Factores múltiples irreducibles.

Deriva formal de un polinomio: Sea $\mathcal{K}$ un anillo de polinomio en x en el cuerpo $\mathcal{F}: \mathcal{K} = \mathcal{F}[x]$. Sea $\mathcal{K}[y]$ una extensión transcendente simple del anillo $\mathcal{K}$ por la adjunción de y. El anillo $\mathcal{K}[y]$será igualmente denotado $\mathcal{F}[x, y]$. Los elementos del anillo $\mathcal{F}[x, y]$. en este caso estos son al igual los elementos del anillo $\mathcal{F}[x]$ denotados $f(x), g(x)$, etc., y si estos son elementos del anillo $\mathcal{F}[y]$. Se denotará $f(y), g(y)$, etc.

Considérese en el anillo $\mathcal{F}[x, y]$ los polinomios

$f(x) = a_0 + a_1 x + . \ . \ . \ a_n x^n \ (a_i \in \boldsymbol{F})$.

$f(y) = a_0 + a_1 y + . \ . \ . \ a_n y^n$.

Así que su diferencia $f(x) - f(y)$. se ve claramente que

$$f(x) - f(y) = \sum_{R=1}^{n} a_R \ (x^R - y^R) =$$

$$= (x - y) \sum_{R=1}^{n} a_R \ (x^{R-1} + x^{R-2} y + . \ . \ . \ . + y^{R-1}) =$$

$$= (x - y) \phi(x, y),$$

donde

$$\phi(x, y) = \sum_{R=1}^{n} a_R \ (x^{R-1} + x^{R-2} y + . \ . \ . \ . + y^{R-1})$$

Nótese que

$$\phi(x,y)=\sum_{R=1}^{n} k\,a_R x^{R-1}=a_1+2a_2x+\ .\ .\ .\ na_nx^{n-1.}$$

DEFINICIÓN. Sea $f=a_0+a_1x+.\ .\ .\ .+a_nx^n$ un polinomio en el cuerpo $\mathcal{F}$. El polinomio

$$\phi(x,y)=\sum_{R=1}^{n} k\,a_R x^{R-1}=a_1+2a_2x+\ .\ .\ .\ n\,a_nx^{n-1.}$$

se le denomina derivada formal de un polinomio f (o polinomio derivado) y se denota f' o $f'(x)$.

TEOREMA 4.1. Sea $\mathcal{F}[x]$ un anillo de polinomios en el cuerpo $\mathcal{F}, f, g$ de los polinomios cualesquiera de $F[x]$ y $\lambda \in F$; entonces se obtiene

(1) $(f+g)'=f'+g'$;
(2) $(fg)'=fg'+f'g$;
(3) $(\lambda f)'=\lambda f'$;
(4) $(f^m)'=mf^{m-1}f'$ para todo m natural.

Demostración. (1) Sea $h=f+g$; entonces

$f(x)-f(y)=(x-y)\phi(x.y), g(x)-g(y)=(x-\mathrm{y})G(x,y)$

$$h(x)-h(y)=f(x)-f(y)+g(x)-g(y)=(x-y)[\phi(x,y)+G(x,y)].$$

Entonces, $h'=\phi(x,x)+G(x,x)=f'+g'$; por tanto

$f+g)'=f'+g'$.

(2) Plantéese $\varphi=fg$, entonces

$$\varphi(x)-\varphi(y)=f(x)g(x)-f(y)g(y)=$$

$$=f(x)\big(g(x)-g(y)\big)+g(y)\big(f(x)-f(y)\big)=$$

$$=(x-y)[f(x)G(x,y)+g(y)\phi(x,y)]$$

De ahi se obtiene

$$\varphi'=f(x)G(x,x)+g(x)\phi(x,x)=f(x)g'(x)+g(x)f'(x);$$

Por consiguiente, $(fg)'=fg'+f'g$.

(3) La fórmula (3) se deduce directamente de la formula (2) para $g=\lambda$, ya que en este caso $g'=0$.

(4) La demostración de la formula (4) se efectúa por deducción en m en la formula (2). □

Descomposición de un polinomio según las potencias de la diferencia $x-c$. Con la división del polinomio $f=a_0x^n+.\ .\ .\ .\ .\ .+a_n$ por un binomio de la forma $x-c$, es fácil obtener los cálculos siguiendo un esquema (llamado *esquema de Horner):*

	a_0	a_1	a_2	. . .	a_{n-1}	a_n

c	b_0	b_1	b_2	$\ldots$	b_{n-1}	r
	a_0	$cb_0 + a_1$	$cb_1 + a_2$	$\ldots$	$cb_{n-2} + a_{n-1}$	$cb_{n-1} + a_n$

Aparentemente, $a_0 = b_0$ cualquier coeficiente seguido del cociente y la resta r se calculan por las fórmulas

$$b_R = cb_{R-1} + a_R (k = 1,\ldots, n-1); r = cb_{n-1} + a_n.$$

Estas fórmulas se obtienen a partir de la igualdad

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = (x - c)(b_0x^{n-1} + b_1x^{n-2} + \ldots b_{n-1}) + r,$$

después de haber eliminado los paréntesis, reducido los términos semejantes e iguales los unos con otros coeficientes asociados en las mismas potencias en los dos miembros de la igualdad

El esquema de Horner es útil para efectuar una descomposición de un polinomio dado f según las potencias del binomio $x - c$.

Sean

$$f = (x - c)q_1 + r_o.$$

$$q_1 = (x - c)q_2 + r_1,.$$

(1) . . . . . .

$$q_{n-2} = (x - c)q_{n-1} + r_{n-2}.$$

$$q_{n-1} = (x - c)a_0 - r_{n-1}.$$

donde q_R y r_R designa el cociente y la resta obtenida después de la división de q_{k-1}por $x - c$. Si la última expresión en (1) de q_{R-1}presentada en la igualdad anterior, luego, la cantidad así obtenida es sustituida en q_{R-2}, etc., obteniéndose la igualdad

(2) $f = r_0 + r_1(x - c) + r_2(x - c)^2 + \ldots + r_{n-1}(x - c)^{n-1} + a_0(x - c)^n.$

Esta, es precisamente, la descomposición del polinomio dado f en potencias de $(x - c)$. Se derivan los dos miembros de la igualdad (2) y plantéese $x = c$ se obtiene

$$f = (c)r_0,\ j'(c) = r_1,\quad f''(c) = 2!\ r_2,\ldots f^{(n)}(c)n!\, a_0.$$

También la igualdad (2) se puede escribirse bajo la forma

$$f = f(c) + f'(c)(x - c) = \frac{f''(c)}{2!}(x - c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x - c)^n$$

si y sólo f es un polinomio en un cuerpo de característica nula. Es esta, precisamente, la *formula de Taylor* para los polinomios. La división siguiendo el esquema de Horner de $f$por $x - c$ abástese los coeficientes del cociente $q_1$que hacen falta dividirlos por $x - c$, etc.; es fácil de obtener todos los cálculos en forma de una tabla.

	a_0	a_1	$\ldots$	a_{n-1}	a_n

c	b_0	b_1	. . .	b_{n-1}	r_0
	c_0	c_1	. . .	r_1	
	d_0	d_1	. . .		
	. . . . .	. . . . .	. . .		. . . . .
	a_0	r_{n-1}			$r_{n-1} = \frac{f^{(n-1)}(c)}{(n-1)!}$

Factores múltiples irreducibles de un polinomio. Sea $\mathcal{F}(x)$ un anillo de polinomios en el cuerpo $\mathcal{F}$ de característica nula.

DEFINICIÓN: Sea $\mathcal{F}$ un polinomio de $F(x)$y p su factor irreducible. Se denomina *factor de multiplicidad m (o factor múltiple de orden m)*del polinomio$f$el polinomio p si

(1) $f = p^m g, \qquad p \dagger g, \qquad g \in F[x].$

Para $m > 1$ el polinomio p se llama factor múltiple y para $m = 1$ factor primo del polinomio f.

TEOREMA 4.3. Sea $\mathcal{F}(x)$ un anillo de polinomio en el cuerpo $\mathcal{F}$ de característica nula y $f \in F[x]$. Sea p un *factor irreducible de multiplicidad$m \geq 1$* del polinomio$f$. p es entonces un factor de multiplicidad $m - 1$de la función f'.

Demostración. Por hipótesis, p es un factor múltiple de orden m del polinomio f y por consiguiente, la condición (1) se satisface. Sirviéndose de las propiedades de la derivada, se obtiene

$$f' = mp^{m-1}p'g + p^m g',$$

(2) $f' = p^{m-1}(mp'g + pg'),$

Dado que por hipótesis el cuerpo $\mathcal{F}$ tiene una característica nula, se tiene $mp' = 0$ y $\operatorname{grad}(mp') < \operatorname{grad} p$;entonces $p \dagger mp'$. siendo p un polinomio irreducible y (en razón de (1)) $p \dagger g$, se deduce $p \dagger (mp')g$, entonces

(3) $p \dagger (mp'g + pg')$.

En la base de (2) y (3) se concluye que p es u factor de multiplicidad $m - 1$ de la función f'. □

COROLARIO 4.4. *El polinomio f de $\mathcal{F}[x]$ posee factores múltiples irreducibles si y solo si el máximo común divisor de los polinomios f y f' son de grado positivo.*

Raíces múltiples de un polinomio: Sea $\mathcal{F}[x]$ un anillo de polinomio en el cuerpo $\mathcal{F}$ y $\mathcal{F}[x]$ su conjunto de base.

DEFINICIÓN. Sea f un polinomio de $\mathcal{F}[x]$ y c su raíz en $\mathcal{F}$. El elemento c se denomina raíz de multiplicidad m (o raíz múltiple de orden $\boldsymbol{m}$)si $f = (x - c)^m g, g(c) \neq 0, g \in F[x]$; para $m > 1$ el elemento c se llama raíz múltiple y para $m = 1$ se denomina raíz simple del polinomio f.

PROPOSICIÓN 4.5. Sea $\mathcal{F}[x]$ un anillo de polinomio en el cuerpo de característica nula y $f \in F[x]$. El elemento c de F es una raíz múltiple del polinomio f si y solo si $f(c) = f'(c) = 0$.

Esta proposición se deriva directamente del TEOREMA 1.9 y del corolario 4.4.

PROPOSICIÓN 4.6. Sea $\mathcal{F}[x]$ un anillo de polinomios en el cuerpo $\mathcal{F}$ de característica nula y $f \in F[x]$. El elemento $c$es una raíz múltiple de orden m del polinomio f si y sólo si

(1) $f(c) = f'(c) = . . . = f^{(m-1)}(c) = 0, f^{(m)}(c) \neq 0.$

Demostración. Según el TEOREMA 4.3, el elemento c es una raíz múltiple de orden m del polinomio f (es decir $(x - c)$ es un factor múltiple de orden m del polinomio f) si y sólo si

(2) $(x-c)$ divide$f, f'. \ldots . , f^{(m-1)}$ y $(x-c) \dagger f^{(m)}$

Conforme al TEOREMA de Bézout las condiciones (1) y (2) son equivalentes. □

Ejercicios

1. Descomponer el polinomio $x^6 - 5x^5 + 3x^3 - 1$ en potencia de $x - 1$.
2. Descomponer el polinomio $x^5 + 4x^4 - x^3 - 29x^2 - 14x - 1$ en potencia de la diferencia $x - 2$.
3. Descomponer el polinomio $x^5 - x^3 + 1$ en potencia de $x + i$.
4. Calcular los valores del polinomio $x^4 + 3x^2 - 5x + 1$ y de sus funciones para $x = -1$.
5. Determinar la multiplicidad de la raíz 1 del polinomio $x^6 - x^5 - x^4 + 2x^3 - x^2 - x + 1$.
6. Determinar la multiplicidad de la raíz i del polinomio $x^6 + x^5 + 3x^4 + 2x^3 + +3x^2 + 1$.
7. Determinar los coeficientes a y b de manera que el polinomio $ax^4 + bx^3 + 1$ de $\boldsymbol{Q}[x]$ sea divisible por $(x-1)^2$.
8. Determinar los coeficientes a y b de manera que el polinomio $ax^{n+1} + bx^n + 1$ de $\boldsymbol{Q}[x]$ sea divisible por $(x-1)^2$.
9. Determinar el coeficiente a de manera que el polinomio $x^5 - ax^2 - ax + 1$ de $\boldsymbol{Q}[x]$ admite -1 para raíz de multiplicidad no inferior a 2.
10. Buscar en cuales condiciones el polinomio $x^5 + ax^3 + b$ posee en los cuerpos de los números complejos una raíz doble distinta a cero.
11. El polinomio $x^n + a$, donde n es un número natural y a un número no nulo, ¿tiene éste raíces múltiples en el cuerpo de números complejos?
12. Demostrar que el polinomio $1 + \frac{x}{1!} + \frac{x^2}{2!} + . \ . \ . + \frac{x^n}{n!}$ despojado de raíces múltiples en todos los cuerpos numéricos.
13. Sea $\mathcal{F}$ y $\mathcal{P}$ los cuerpos numéricos, siendo $\mathcal{F}$ un sub cuerpo del cuerpo $\mathcal{P}$. Demostrar que si el polinomio f es irreducible en el anillo de los polinomios $\mathcal{F}[x]$, es despojado de factores múltiples en el anillo $\mathcal{P}[x]$.

CAPITULO XV
POLINOMIOS PARA MUCHAS VARIABLES

§ 1. Anillos de polinomios para muchas variables

Extensión múltiple de anillo. Sea $\mathcal{K}$ un sub-anillo íntegro del anillo conmutativo $\mathcal{L}$ y $x_1, \ldots , x_m$ de los elementos del anillo L.

DEFINICIÓN. Una extensión mínima del anillo $\mathcal{K}$ quien es un sub-anillo del anillo $\mathcal{L}$ y contiene los elementos $x_1, \ldots , x_m$ de$\mathcal{L}$, es denominado *sub-anillo del anillo* $\mathcal{L}$ derivado del anillo $\mathcal{K}$ y los elementos $x_1, \ldots , x_m$.

Este anillo es figurado $\mathcal{K}\ [x_1, \ldots , x_m]$ y su conjunto de base, $K\ [x_1, \ldots , x_m]$.

El anillo $\mathcal{K}\ [x_1, \ldots , x_m]$ es aparentemente una intersección de todos los sub-anillos del anillo $\mathcal{L}$ que contiene los elementos $x_1, \ldots , x_m$ y teniendo el anillo $\mathcal{K}$ en calidad de sub-anillo.

DEFINICIÓN. Un anillo figurado $\mathcal{K}\ [x_1]. \ . \ [x_m]$ es definido por inducción a medida de las fórmulas

$$\mathcal{K}\ [x_1][x_2] = (\mathcal{K}[x_1])\ [x_2],$$

$$\mathcal{K}\ [x_1][x_2]. \ . \ . \ [x_m] = (\mathcal{K}\ [x_1][x_2]. \ . \ . \ [x_{m-1}])[x_m],$$

se denomina *extensión múltiple de orden m del anillo* $\mathcal{K}$.

TEOREMA: 1.1 *sea* $\mathcal{K}$ *un sub anillo del anillo conmutativo* $\mathcal{L}$ *y* $x_1, \ldots , x_m \in L$; *entonces*

(1) $\mathcal{K}\,[x_1\ x_2,\ldots,\ x_{m-1}] = \mathcal{K}\,[x_1][x_2].\ldots[x_m]$.

Demostración. El TEOREMA es aparentemente verdadero para $m = 1$. Supóngase que el TEOREMA es verdadero cuando agregamos $m-1$ elementos para el anillo $\mathcal{K}$. Por definición, se tiene

$K[x_1,\ldots,x_{m-1}] \subset K\,[x_1,\ldots,x_m]$ y $x_m \in K\,[x_1,\ldots,x_m]$,

también se tiene

(2) $(k\,[x_1,\ldots.x_{m-1}])[x_m] \subset K\,[x_1,\ldots.,\ x_m]$.

Por otra parte, ya que $x_1,\ldots,x_m \in (K\,[x_1,\ldots.,\ x_m])[x_m]$, se tiene

(3) $k\,[x_1,\ldots.x_{m-1}] \subset (K\,[x_1\ x_2,\ldots,\ x_{m-1}]\,)[x_m]$.

En virtud de (2) y (3), resulta

(4) $K\,[x_1,\ldots,x_{m-1,}\,x_m] = K[x_1,\ldots,x_{m-1}][x_m]$.

Por hipótesis de recurrencia, se tiene

(5) $K[x_1,\ldots,x_{m-1}] = K[x_1].\ldots[x_{m-1}]$.

Sobre la base de las igualdades (4) y (5), se concluye que

$K[x_{1,}\,x_2,\ldots,x_m] = K[x_1][x_2]\ldots[x_m]$.

Por consiguiente, la formula (1) es verdadera. □

Anillo de los polinomios para muchas variables. Sea m un entero positivo y N un conjunto de todos los números naturales. Sea $\mathrm{N}^1 = \mathrm{N}$ y para $m > 1$

$\mathrm{N}^m = \{\,(i_1,\ldots,i_m) \mid i_1,\ldots,i_m \in \mathrm{N}\,\}$,

donde $(i_1,\ldots,i_m)$ es un vector para m dimensiones.

Según el TEOREMA 1.1, $\mathcal{K}\,[x_1,\ x_2] = (\mathcal{K}\,[x_1])[x_2]$. También, los elementos del anillo $\mathcal{K}\,[x_1,\ x_2]$ estos constituyen una suma de la forma

$\propto_0 + \propto_1 x_2 + \ldots + \propto_n x_2^n$,

donde $\propto_i = \propto_{i0} + a_{i1}x_1 + \ldots + a_{im}x_1^m$ $(a_{ir} \in K)$, y m es la potencia más elevada de los polinomios $\propto_0, \propto_1, \ldots, \propto_n$. Así que los elementos del anillo $\mathcal{K}[x_1,\ x_2]$ pueden ser escritos bajo la misma forma

$\sum_{(i_1,i_2)\in M} a_{i1i2}x_1^{i_1}x_2^{i_2}$ $\qquad\qquad$ $\left(a_{i_1i_2} \in K\right)$,

donde Mes un sub-conjunto finito no vacío del conjunto $\mathrm{N}^2 = \mathrm{N} \times \mathrm{N}$. Basándose en el TEOREMA 1.1, concluimos de la misma manera que los elementos del anillo $\mathcal{K}\,[x_1,\ldots,x_m]$ son una suma de la forma

$\sum_{(i_1,\ldots,i_m)\in M} a_{i_1,\ldots i_m} x_1^{i_1}\ldots x_m^{i_m}$,

donde M Mes un sub-conjunto finito no vacío del conjunto N^m y $a_{i_1\ldots i_m} \in K$. Se escribirá esta suma forma bajo la forma plasmada

$\sum_{(i)\in M} a_{(i)} x_1^{i_1}\ldots x_m^{i_m}$, Donde $(i)=(i_1,\ldots,i_m)$.

Recuérdese que el elemento x_1 del anillo $\mathcal{K}[x_1]$ es llamado transcendente sobre $\mathcal{K}$ si para todos los elementos $a_1, \ldots, a_n$ del anillo $\mathcal{K}$ de la igualdad

$\sum_{i=1}^{n} a_i x_1^i = 0$ Siguiendo las igualdades $a_1 = 0, \ldots, a_n = 0$.

La generalización de esta noción es la noción de la independencia algebraica de la colección de los elementosx_1, $\ldots, x_m$ sobre $\mathcal{K}$.

Sea $\mathcal{K}$ un sub-anillo del anillo conmutativo$\mathcal{L}$.

DEFINICIÓN: Los elementos $x_1,\ldots,x_m$del anillo $\mathcal{L}$ se denominan *algebraicamente independientes* o simplemente *algebraicos sobre el anillo* $\mathcal{K}$si para todos los elementos (a_i) del anillo $\mathcal{K}$ de la igualdad

(I) $\sum_{(I)\in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m} = 0$, donde $M \subset \mathrm{N}^m$,

se deduce la igualdad a cero de todos los coeficientes $a_{(i)}$.

Para $m = 1$ se obtiene como resultado la definición de elementos algebraicos independientes (o algebraico) sobre $\mathcal{K}$ que coincide con la definición del elemento transcendente sobre $\mathcal{K}$.

TEOREMA 1.2. *Sea $\mathcal{K}$ un sub-anillo del anillo conmutativo $\mathcal{L}$ y $x_1,\ldots,x_m \in L$. Los elementos $x_1,\ldots,x_m$ son algebraicos sobre $\mathcal{K}$ si y solo si para cada $s \in \{1,\ldots,m\}$el elemento x_s es transcendente sobre $\mathcal{K}[x_1,\ldots,x_{s-1}]$.*

Demostración. Supóngase que los elementos $x_1,\ldots,x_m$ son algebraicos sobre $\mathcal{K}$ y demuéstrese que para cada $s \in \{1,\ldots,m\}$ el elemento x_s es transcendente sobre el anillo $\mathcal{K}[x_1,\ldots,x_{s-1}]$.

Sea

(II) $A_0 + A_1 x_s + \ldots + A_l x_s^l = 0$, donde $A_R \in K[x_1,\ldots,x_{s-1}]$. Los términos $A_R x_s^R$ pueden tomar la forma

$A_R x_s^R = \sum_{(i)\in M_R} a_{(i)} x_1^{i_1}\ldots x_{s-1}^{i_{s-1}} x_s^R x_{s+1}^0 \ldots x_m^0$, Donde $M_R \subset \mathrm{N}^m$,

Entonces, la igualdad (ll) puede plasmarse así

(3) $\sum_{(i)\in \cup M_R} a_{(i)} x_1^{i_1}\ldots x_s^{i_s} x_{s+1}^0 \ldots x_m^0 = 0$

En virtud de la independencia algebraica de los elementos $x_1,\ldots,x_m$ sobre el anillo $\mathcal{K}$ se deduce de (3) la igualdad a cero de todos los coeficientes $a_{(i)}$ por $(i) \in \cup M_R$ así que $A_R = 0$ para $K = o, 1, \ldots, l$. Por consiguiente para cada $s \in \{1,\ldots,m\}$ el elemento x_s es transcendente sobre $\mathcal{K}[x_1,\ldots,x_{s-1}]$.

Supóngase que para cada $S \in \{1,\ldots,m\}$ el elemento x_s es trascendente sobre $\mathcal{K}[x_1,\ldots,x_{s-1}]$ Y demuéstrese por recurrencia sobre m que dé (I) se deduce la igualdad a cero de todos los coeficientes $a_{(i)}$.

Para $m = 1$ la afirmación es aparentemente verdadera. Admítase que la afirmación es verdadera para la colección de los elementos $x_1, \ldots, x_{m-1}$. Escríbase la igualdad (I) bajo la forma

(4) $A_0 + A_1 x_m + A_2 x_m^2 + \ldots + A_r x_m^r = 0$

donde

$A_R x_m^R = \sum_{(i)(i)\in M_R} a_{(i)} x_1^{i_1} \ldots x_{m-1}^{i_{m-1}} x_m^R$,

$A_R \in K\,[x_1, \ldots, x_{m-1}]$, $\qquad M = \overset{\cup}{R}\, M_R$.

Por hipótesis el elemento $x_m$es trascendente sobre $\mathcal{K}\,[x_1, \ldots, x_{m-1}]$, asi que de (4) siguiendo las igualdades $A_0 = 0$, $A_1 = 0, \ldots, A_r = 0$. Por hipótesis de recurrencia siguiendo las igualdades

$a_{(i)} = 0$ Para $(i) \in \cup\, M_R = M$.

Por consiguiente los elementos $x_1, \ldots, x_m$ son algebraicos sobre $\mathcal{K}$. □

Sea $\mathcal{K}$ un anillo conmutativo íntegro y $\mathcal{K}\,[x_1] \ldots [x_m]$ una extensión múltiple de orden k del anillo $\mathcal{K}$ por adjunción de los elementos $x_1, \ldots, x_m$. Según el TEOREMA 1.1, $\mathcal{K}\,[x_1, \ldots, x_m] = \mathcal{K}[x_1] \ldots [x_m]$ y seguido del anillo $[x_1, \ldots, x_m]$ es de igual manera una extensión múltiple de orden k del anillo $\mathcal{K}$.

DEFINICIÓN. El anillo $\mathcal{K}\,[x_1, \ldots, x_m]$ se denomina *extensión transcendente múltiple de orden* m del anillo $\mathcal{K}$ si para todo $s \in \{1, \ldots, m\}$el anillo $\mathcal{K}\,[x_1, \ldots, x_s]$ es una extensión trascendente simple del anillo $\mathcal{K}\,[x_1, \ldots, x_{s-1}]$ por adjunción de x_s.

Señálese que para $m = 1$ la extensión trascendente múltiple de orden del anillo $\mathcal{K}$ es una extensión trascendente simple del anillo $\mathcal{K}$.

TEOREMA 1.3. *Sea $\mathcal{K}$ un anillo conmutativo no reducido para $\{0\}$. Para todo m natural diferente de cero existe una extensión transcendente múltiple de orden m del anillo $\mathcal{K}$. Además si $\mathcal{K}$ es un dominio de integridad entonces la extensión transcendente múltiple de orden m de este anillo igualmente constituye un dominio de integridad.*

Demostración. Apoyándose en el TEOREMA 14.1.2 sobre la existencia de una extensión transcendente simple de un anillo, se esta apto para construir sucesiva de los anillos:

$\mathcal{K}\,[x_1]$

$(\mathcal{K}[x_1])[x_2]$,

. . . . . .

$(\mathcal{K}\,[x_1] \ldots [x_{m-1}])[x_m]$,

donde $\mathcal{K}\,[x_1]$ es una extensión transcendente simple del anillo $\mathcal{K}$ por adjunción de x_1, $(\mathcal{K}[x_1])[x_2]$ una extensión transcendente simple del anillo $\mathcal{K}\,[x_1]$ por adjunción de x_2. Etc. En fin, $(\mathcal{K}\,[x_1] \ldots [x_{m-1}])[x_m]$ una extensión transcendente simple del anillo $\mathcal{K}\,[x_1] \ldots [x_{m-1}]$ por adjunción de x_m. Por definición precedente el TEOREMA este último anillo es una extensión trascendente múltiple de orden m del anillo $\mathcal{K}$. Además, según el TEOREMA 14.1.6 si $\mathcal{K}$ es un dominio de integridad todos los anillos construidos más adelantes son de dominios de integridad.

DEFINICIÓN. El anillo, $\mathcal{K}\,[x_1, \ldots, x_m]$ constituye una extensión trascendente múltiple de orden m de un anillo conmutativo integro $\mathcal{K}$ es llamado *anillo de los polinomios sobre $\mathcal{K}$ en $x_1, \ldots, x_m$.*

Algunas veces son necesario los elementos $f, g,$ etc., son igualmente señalados $f(x_1,\ldots,x_m)$, $g\ (x_1,\ldots,x_m)$, *etc.*

Isomorfismos de anillos de los polinomios. Sea $\mathcal{K}$ y $\mathcal{L}$ de los anillos conmutativos íntegros.

TEOREMA 1.4 *sea* $\mathcal{K}$ *y* $\mathcal{L}$ *de los anillos isomorfos y* φ *un isomorfismo de* $\mathcal{K}$ *sobre* $\mathcal{L}$, $\mathcal{K}[x_1,\ldots,x_n]$, *y* $\mathcal{L}[y_1,\ldots,y_n]$ *que son anillos de polinomios. Existe un isomorfismo del anillo* $\mathcal{K}[x_1,\ldots,x_n]$ *sobre el anillo* $\mathcal{L}[y_1,\ldots,y_n]$ *que reemplaza* $x_1,\ldots,x_n$ *en* $y_1,\ldots,y_n$ *respectivamente prolongando el isomorfismo* φ.

Demostración. Efectúese la recurrencia sobre n. Si $n=1$ entonces según el TEOREMA 14.1.2 existe un isomorfismo $\varphi_1\ del\ anillo\ \ \mathcal{K}[x_1]$ sobre el anillo $\mathcal{L}[y_1]$ tal como $\varphi_1(x_1)=y_1$ y $\varphi_1(a)=\varphi(a)$ para todo elemento $a\ de\ k$.

Admítase que existe un isomorfismo φ_n del anillo $\mathcal{K}[x_1,\ldots,x_n]$ sobre el anillo $\mathcal{L}[y_1,\ldots,y_n]$ que reemplaza $x_1,\ldots,x_n$ en $y_1,\ldots,y_n$ respectivamente y que prolonga el isomorfismo φ. Entonces según el TEOREMA 14.1.2 existe un isomorfismo φ_n+1 del anillo $(\mathcal{K}[x_1,\ldots,x_n])[x_{n+1}]$ sobre el anillo $(\mathcal{L}[y_1,\ldots,y_n])[y_{n+1}]$ reemplazando x_{n+1} en y_{n+1} y prolongando el isomorfismo φ_n. Teniendo en cuenta el TEOREMA 1.1,

$$(\mathcal{K}[x_1,\ldots,x_n])[x_{n+1}]=\mathcal{K}[x_1,\ldots,x_{n+1}]\ \text{Y}$$

$$(\mathcal{L}[y_1,\ldots,y_n])[y_{n+1}]=\mathcal{L}[y_1,\ldots,y_{n+1}]$$

Se concluyó que φ_{n+1} es un isomorfismo de $\mathcal{K}[x_1,\ldots,x_{n+1}]$ sobre $\mathcal{L}[y_1,\ldots,y_{n+1}]$ que reemplaza los elementos $x_1,\ldots,x_{n+1}$ en $y_1,\ldots,y_{n+1}$ respectivamente y que prolonga el isomorfismo φ.

Así la afirmación del TEOREMA es verdadera para cualquier número natural n.□

COROLARIO 1.5. *Sea* $\mathcal{K}[x_1,\ldots,x_n]$ *y* $\mathcal{K}[y_1,\ldots,y_n]$ *anillos de los polinomios sobre el anillo* $\mathcal{K}$. *Existe entonces un isomorfismo* φ *del anillo* $\mathcal{K}[x_1,\ldots,x_n]$ *sobre el anillo* $\mathcal{K}[y_1,\ldots,y_n]$ *que sustituye* $x_1,\ldots,x_n$ *en* $y_1,\ldots,y_n$ *respectivamente y tal como* $\varphi(a)=a$ *para todo elemento del anillo* $\mathcal{K}$.

Representación normal de un polinomio y grado de un polinomio. Sea $\mathbf{N}$ un conjunto de todos los números naturales y m un número natural fijo diferente de cero. Para todo número natural k defínase el conjunto S_R:

$S_R=\{(i_1,\ \ldots,i_m)\in \mathrm{N}^R \mid i_1+\ldots+i_m=k\}$.

Nótese que

(1) $S_i\cap S_R=\emptyset$ para $l\neq k$.

El polinomio $\sum_{(i)\in M} a_{(i)}x_1^{i_1}\ldots x_m^{i_m}$ se denomina *nulo* si todos los coeficientes $a_{(i)}$ son nulos.

TEOREMA 1.6. *Sea* f *un polinomio no nulo del anillo de los polinomios* $\mathcal{K}[x_1,\ldots,x_m]$. *Existe para el polinomio* f *un numero natural* n *y una representación tal como*

(2) $f=\sum_{R=0}^{n}\left(\sum_{(i)\in S_R} a_{(i)}x_1^{i_1}\ldots x_m^{i_m}\right)$, donde $f\in K$,

para lo cual al menos un coeficiente $a_{(i)}$ *no nulo verifica la relación* $i_1+\ldots+i_m=n$. *Esta representación es única en ese sentido que si*

(3) $f=\sum_{R=0}^{n}\left(\sum_{(i)\in S_R} b_{(i)}x_1^{i_1}\ldots x_m^{i_m}\right)$, *donde* $b_{(i)}\in K$,

es otra representación entonces obtenemos $s = n$ *y* $a_{(i)} = b_{(i)}$*para todos los* (i) *de* S_R *con* $k = 0, 1, \ldots, n$

Demostración. Sea

(4) $f = \sum_{(i)\in M}^{n}, a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$ $(a_i \in K)$,

donde M es un sub-conjunto finito del conjunto N^m. No hay en esta suma términos parecidos y ya que f es un polinomio no nulo, existe en la suma (4) de los coeficientes no nulos. El conjunto M que son finito, hay un número natural n que satisface a las condiciones

$$a_{i_1 \ldots, i_m} \neq 0, \qquad i_1 + \ldots + i_m = n.$$

y

Si $a_{R_1 \ldots} R_m \neq 0$, entonces $k_1 + \ldots + k_m \leq n$ para todo

$$(k_1, \ldots, k_m) \in M.$$

Sea $M^* = \bigcup_{R=0}^{n} S_R$. Supóngase

$a_{(i)} = 0$ Para $(i) \in M^* \setminus M$

Al apoyarse en (4), se concluye que

(5) $f = \sum_{(i)\epsilon M*} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$.

Como $M^* = \bigcup_{R=0}^{n} S_R$ y $S_1 \cap S_R = \emptyset$ para $l \neq k$. Se deduce de (5) la representación (2)

Admítase que para una representación (2) existe una representación (3). Si $m < n$, sustrayendo la igualdad (2) y (3), resulta

(6) $\sum_{(i)\in S_n} a(i) x_1^{i_n} \ldots x_m^{i_m} + \ldots + \sum_{R=0}^{m} \left(\sum_{(i)\in S_R} \left(a_{(i)} - b_{(i)}\right) x_1^{i_n} \ldots x_m^{i_m} \right) = 0.$

En virtud de la independencia algebraica de los elementos $x_1, \ldots, x_m$ todos los coeficientes en (6) son nulos y en particular

$a_{(i)} = 0$ Para todos $(i) \in S_n$,

lo que es una contradicción con la hipótesis del TEOREMA. De manera análoga, se convence de la hipótesis de la imposibilidad de la desigualdad $n < m$, por lo tanto $m = n$. Así, la igualdad (6) puede plasmarse bajo la forma

(7) $\sum_{R=0}^{n} \left(\sum_{(i)\in S_R} \left(a_{(i)} - b_{(i)}\right) x_1^{i_1} \ldots x_m^{i_m} \right) = 0.$

En virtud de la independencia algebraica de $x_1, \ldots, x_m$ se deduce de (7) que $a_{(i)} = b_{(i)}$ para todos los $(i) \in S_R$, donde $k = \{0, 1, \ldots, n\}$.

La representación (2) del TEOREMA 1.6 es *denominada representación normal del polinomio*.

DEFINICIÓN. Se denomina *grado de monomio* $a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$, cuyo coeficiente $a_{(i)}$ no es nulo, la suma $i_1 + \ldots + i_m$.

DEFINICIÓN. Se denomina *grado de un polinomio* f no nulo, $f \in K\,[x_1, \ldots, x_m]$ el más grande de los monomios no nulos entrando en la representación normal del polinomio f.

El grado del polinomio nulo no está definido. El grado del polinomio f se manifiesta con símbolo grad f.

DEFINICIÓN. un polinomio f de grado n se llama *homogéneo* si

$$f = \sum_{i_1+\ldots i_{m=n}} a_{(i)}\, x_1^{i_1} \ldots x_m^{i_m}.$$

Un polinomio homogéneo del primer grado se denomina *polinomio lineal.*

Nótese las propiedades más importantes del grado de un polinomio.

TEOREMA 1.7. Siendo f y g dos polinomios cualquieras del anillo de los polinomios $\mathcal{K}\,[x_1, \ldots, x_m]$. Se tiene entonces:

(1) Si $f + g \neq 0$, entonces grad $(f + g) \leq \max\{\text{grad}\, f, \text{grad g}\}$;
(2) Si $f.g$ *es un polinomio no nulo, entonces grad* $(fg) \leq$ grad f +grad g;
(3) Si $\mathcal{K}$ *es un dominio de integridad, entonces grad* $(fg) = \text{grad}\, f + \text{grad g}$.

La demostración del TEOREMA 1.7 se deja en manos del lector.

Anillo de polinomio factorial. Demuéstrese un TEOREMA análogo en un TEOREMA 14.3.7

TEOREMA 1.8. *Sea* $\mathcal{K}$ *un anillo factorial. Entonces el anillo de los polinomios* $\mathcal{K}[x_1, \ldots, x_m]$ *en* $x_1, \ldots, x_n$ *sobre* $\mathcal{K}$ *también es un anillo factorial.*

Demostración. El TEOREMA se demuestra por recurrencia sobre n. Por $n = 1$ la afirmación es verdadera según el TEOREMA 14.3.7. Admítase que el anillo de los polinomios $\mathcal{K}[x_1, \ldots, x_{n-1}]$ en $x_1, \ldots, x_{n-1}$ sobre $\mathcal{K}$ es factorial. Demuéstrese entonces que es igualmente factorial el anillo $[x_1, \ldots, x_n]$. Según el TEOREMA 1.1,

$$\mathcal{K}\,[x_1, \ldots, x_n] = \mathcal{K}[x_1] \ldots [x_n] = (\mathcal{K}[x_1] \ldots [x_{n-1}])[x_n] = (\mathcal{K}\,[x_1, \ldots, x_{n-1}])[x_n].$$

Por hipótesis de deducción el anillo $\mathcal{K}\,[x_1, \ldots, x_{n-1}]$ es factorial. Por consiguiente en virtud del TEOREMA 14.3.7 es factorial su extensión $(\mathcal{K}[x_1, \ldots, x_{n-1}])[x_n]$ por adjunción del elemento x_n transcendente sobre el anillo $\mathcal{K}\,[x_1, \ldots, x_{n-1}]$. Como también el anillo de los polinomios $\mathcal{K}\,[x_1, \ldots, x_n]$ es factorial para todo n natural.□

COROLARIO 1.9. *Un anillo de los polinomios* $\mathcal{F}\,[x_1, \ldots, x_{n-1}]$ *sobre el cuerpo* $\mathcal{F}$ *es factorial.*

Ejercicios:

1. Mostrar que los polinomios siguientes para dos variables son irreductibles sobre el cuerpo de los números racionales: (a) $3_{x^2} - \text{y}$: $(b)\ x^2 + y^2 - 1$. ¿Son estos polinomios reductibles sobre un cuerpo de los números complexos?
2. Demostrar que un anillo de los polinomios $\mathcal{F}\,[x, y]$ sobre el cuerpo $\mathcal{F}$ para dos variables no constituyen de ideales principales.
3. Sea $\mathcal{F}\,[x, y]$ un anillo de los polinomios sobre el cuerpo $\mathcal{F}$ para dos variables. demostrar que el anillo cociente $\mathcal{F}\,[x, y]$ / $(x - y)$ es isomorfa al anillo $\mathcal{F}\,[x]$.

§2. Polinomios simétricos

Orden lexicográfico de los términos de un polinomio. Sea N un conjunto de todos los números naturales y m un número natural fijo diferente de cero. Los conjuntos del elemento N^m son vectores para m dimensiones a los elementos naturales. Sea

$$i = (i_1, \ldots, i_m), \qquad K = (k_1, \ldots, k_m).$$

Sobre el conjunto N ^{m} introduciéndose un orden lexicográfico estimando, por definición que

(1) $(i_1,\ldots,i_m) < (k_1,\ldots,k_m)$

si es positivo el primer elemento no nulo del vector $(k_1 - i_1,\ldots,k_m - i_m)$. Vamos a decir que el vector i es inferior al vector K. Mientras que el vector K es superior al vector i.

TEOREMA 2.1. *Un orden lexicográfico Sobre un conjunto N ^{m} es una relación de orden lineal estricto.*

Demostración. De la definición del orden lexicográfico se deduce que para dos vectores cualquierai, K de N ^{m} no satisface más que a una de las tres condiciones $i < K, i = K, K < i$.

La relación $<$ sobre el conjunto N ^{m} es transitiva. De hecho, si $i < K$ y $K < 1$, entonces $K - i > 0$, $I - K > 0$, donde $0 = (0,\ldots,0)$. Se deduce que $(K - i) + (i - K) > 0$ y $l - i > 0$, es decir $i < l$.□

COROLARIO 2.2. S*ea M un sub-conjunto finito no vacío del conjunto N^{m}. El orden lexicográfico sobre N^{m} inducido es más un orden lineal estricto sobre M.*

Sean f un polinomio no nulo del anillo de los polinomios $\mathcal{K}[x_1,\ldots,x_m]$ y

(2) $f = \sum_{(i)\in M} a_{(i)} x_1^{i_1}\ldots x_m^{i_m}$

Su representación para coeficientes no nulos, es decir

$a_{(i)} \neq 0$ Para cada $(i) \in M$

Sea S un conjunto de monomios que figuran en f (en la suma (2)). Introdúzcase sobre el conjunto S la relación de orden planteándose

(3) $a_{i_1\ldots i_m} x_1^{i_1}\ldots x_m^{i_m} < a_{R_1\ldots R_m} x_1^{R_1}\ldots x_m^{R_m}$

si y sólo si $(i_1,\ldots,i_m) < (k_1,\ldots,k_m)$. De hecho esta relación binaria es transitiva, anti reflexiva y además lineal. Así que la relación de orden lexicográfico sobre S también es un orden lineal estricto.

DEFINICIÓN. El mayor elemento de un conjunto ordenado $\langle S <\rangle$ se denomina *término director del polinomio f.*

Si la desigualdad (3) está completa, decimos que el término $a_{i_1\ldots i_m} x_1^{i_1}\ldots x_m^{i_m}$ es inferior al término $a_{R_1\ldots R_m} x_1^{R_1}\ldots x_m^{R_m}$. El término director es evidentemente superior a cualquier monomio del polinomio f.

Lema sobre el término director de producto de dos polinomios.

Entonces el estudio de las propiedades de los polinomios simétricos el lema siguiente sea necesario.

LEMA 2.3. Sea $\mathcal{K}[x_1,\ldots,x_m]$ un anillo de los polinomios en $x_1,\ldots,x_m$ sobre el dominio de la integridad $\mathcal{K}$. El término director de producto de dos polinomios no nulos del anillo $\mathcal{K}[x_1,\ldots,x_m]$ es igual al producto de los términos director de los cofactores.

Demostración. Sea f y de$g$ de los polinomios no nulos del anillo considerado $ax_1^{i_1}\ldots x_m^{i_m}$ y $bx_1^{R_1}\ldots x_m^{Rm}$ los términos directores de los polinomios f y g respectivamente. Es necesario demostrar que el término director del polinomio fg es el monomio

(I) $ax_1^{i_1+R_1}\ldots x_m^{i_m+R_m}$.

Nótese que $ab \neq 0$, ya que $\mathcal{K}$ es un dominio de integridad. Sean

(1) $cx_1^{i_1} \ldots x_m^{i_m}\, dx_1^{s_1} \ldots x_m^{s_m}$

todos los términos no nulos en representación normal de los polinomios f y g respectivamente. Se tiene entonces las desigualdades

(2) $(i_1, \ldots, i_m) \leq (i_1, \ldots, i_m)$,
(3) $(s_1, \ldots, s_m) \leq (k_1, \ldots, k_m)$.

Basta demostrar que si al menos una de esas desigualdades es estricta, entonces

(4) $cdx_1^{j_1+s_1} \ldots x_m^{j_m+s_m} < abx_1^{i_1+R_1} \ldots x_m^{i_m+R_m}$.

De hecho, si al menos una de las desigualdades (2) y (3) es estricta, se tiene

(5) $(i_1 - j_1, \ldots, i_m - j_m) > \mathbf{0}$ o $(k_1 - s_1, \ldots, k_m - s_m) > 0$
(6)

Y, en virtud de (2), (3), (5), resulta

(7) $(i_1 - k_1, \ldots, i_m - k_m) - (i_1 + s_1, \ldots, i_m + s_m) > 0$.

De (6) se obtiene (4). La desigualdad (4) se completa para todos los términos no nulos de (1) en representación normal de los polinomios f y g en el que al menos uno no es el termino director de polinomios respectivo. Sobre la base de esos razonamientos se concluye que el monomio (l) es el término director de producto fg. □

Polinomios Simétricos. Sea $\mathcal{K}[x_1, \ldots, x_m]$ un anillo de los polinomios en $x_1, \ldots, x_m$ sobre el anillo conmutativo $\mathcal{K}$. Sea S_m un conjunto de permutación de grado m.

DEFINICIÓN. Un polinomio f de $\mathcal{K}[x_1, \ldots, x_m]$ es llamado *polinomio simétrico* en $x_1, \ldots, x_m$ si para toda permutación $\tau \in S_m$ se obtiene la igualdad

$$f(x_1, \ldots, x_m) = f\left(x_{\tau_{(1)}}, \ldots, x_\tau(m)\right).$$

Ejemplo. El polinomio $x_1^2 + \ldots + x_m^2 + x_1 + x_2 + \ldots + x_m$ llegando a ser la misma para toda permutación de los elementos $x_1, \ldots, x_m$.

DEFINICIÓN. Se denominan *polinomios simétricos elementales en* $x_1, \ldots, x_m$ los polinomios

$\sigma_1 = x_1 + x_2 + \ldots + x_m$;
$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{m-1}x_m$;
. . . . . .
$\sigma_m = x_1x_2 \ldots x_m$

Estos aparecen con el estudio del polinomio $\varphi = (z - x_1)(z - x_2) \ldots (z - x_m)$ igual al polinomio

$$z^m - (x_1 + x_2 + \ldots x_m)z^{m-1} + (x_1x_2 + \ldots x_{m-1}x_m)z^{m-2} + \ldots + (-1)^m x_1 \cdots x_m.$$

Así, $\varphi = z^m - \sigma_1 z^{m-1} + \sigma_2 z^{m-2} - \ldots + (-1)^m \sigma_m$.

Se verifica fácilmente que el conjunto de todos los polinomios simétricos del anillo $\mathcal{K}\,[x_1,\ldots,x_m]$ es un sub anillo de ese anillo; nótesele $S\mathcal{K}\,[x_1,\ldots,x_m]$. Por otra parte los polinomios simétricos elementales en $x_1,\ldots,x_m$ que generan un cierto sub-anillo $\mathcal{K}\,[x_1,\ldots,x_m]$ que se notara en $\mathcal{K}\,[\sigma_1,\ldots,\sigma_2]$. Se constata fácilmente que

$$\mathcal{K}\,[\sigma_1,\ldots,\sigma_m] \prec S\mathcal{K}\,[x_1,\ldots,x_m].$$

¿Coinciden estos dos anillos? Todo polinomio simétrico en $x_1,\ldots,x_m$ ¿Esta se representa bajo la forma de polinomio compuesto de polinomios simétricos elementales $\sigma_1,\ldots,\sigma_m$? Se dará más adelante una respuesta afirmativa a esta pregunta.

Lemas de los polinomios simétricos. Sea $\mathcal{K}\,[x_1,\ldots,x_m]$ un anillo de los polinomios en $x_1,\ldots,x_m$.

LEMA 2.4. Si $ax_1^{R_1}\,x_2^{R_2}\ldots ax_1^{R_m}$ *es el término director de un polinomio simétrico, entonces* $k_1 \geq k_2 \geq \ldots\; k_m$.

Demostración. Sea f un polinomio de$K\,[x_1,\ldots,x_m]$ simétrico con respecto a $x_1,\ldots,x_m$ y

(1) $ax_1^{R_1}\,x_2^{R_2}\ldots ax_1^{R_m}\quad (a\in K)$

el término director de polinomio f. La representación normal del polinomio simétrico f cuenta con los monomios

(2) $ax_1^{R_2}\,x_2^{R_1}x_3^{R_3}\ldots x_m^{R_m}$

(3) $ax_1^{R_1}\,x_2^{R_3}x_3^{R_2}\ldots x_m^{R_m}$

Dado que el monomio (1) es superior al monomio (2) se obtiene $k_1 \geq k_2$. Ya que el monomio (1) es superior al monomio (3) se obtiene $k_2 \geq k_3$, etc. Por consiguiente $k_1 \geq k_2 \geq k_3 \geq \ldots \geq k_m$.

LEMA 2.5. Sea $ax_1^{R_1}\,x_2^{R_2}\ldots ax_1^{R_m}$ *el término director de un polinomio simétrico no nulo* $f\in K\,[x_1,\ldots,x_m]$ *. Entonces los términos directores de polinomios* f *y* $a\sigma_1^{R_{1-R_2}}\sigma_2^{R_2-R_s}\ldots\sigma_m^{R_m}$ *coincidirán.*

Demostración. Se observa fácilmente que los polinomios simétricos elementales $\sigma_1,\ \sigma_2,\ldots,\ \sigma_{m-1},\sigma_m$ se suministran de los términos siguientes:

$$x_1, x_1x_2,\ldots, x_1x_2\ldots x_{m-1}, x_1x_2\ldots x_m.$$

Según el lema sobre el término director de producto de los polinomios los términos director de polinomios

(1) $a\sigma_1^{R_{1-R_2}}\sigma_2^{R_2-R_s}\ldots\sigma_{m-1}^{R_{m-1}-R_m},\sigma_m^{R_m}$

son respectivamente los monomios

$$ax_1^{R_{1-R_2}},(x_1x_2)R_2-R_s,\ldots(x_1x_2\ldots x_{m-1})R_{m-1}-R_m,(x_1\ldots x_m)R_m.$$

En virtud del mismo lema, el producto de esos monomios es el monomio $ax_1^{R_1}x_2^{R_2}\ldots x_m^{R_m}$ es el término director de producto de los polinomios (1). Así, los términos directores de polinomios f y $a\sigma_1^{R_{1-R_2}},\ \ldots\sigma_m^{R_m}$ coinciden. □

Sea $\mathcal{K}\,[x_1,\ldots,x_m]$ un anillo de los polinomios en $x_1,\ldots,x_m$ se introduce sobre el conjunto de los polinomios no nulos de ese anillo, la relación binaria $>$: $f > g$ *si y solo si el termino director de* f *es mayor al termino* g. Se constata sin duda que esta relación de naturalidad lineal.

DEFINICIÓN. La secuencia $\varphi_1,\varphi_2,\varphi_3,\ldots$ de los polinomios de $K\,[x_1,\ldots,x_n]$ es denominada *cadena descendiente* si

(1) $\varphi_1 > \varphi_2 > \varphi_3 > \ldots$

Lema 2.6 *una cadena descendiente de polinomios simétricos no nulos del anillo de los polinomios* $\mathcal{K}\,[x_1,\ldots,x_m]$ *no puede ser infinita*.

Demostración. Sea (19 una cadena descendiente de polinomios simétricos. El término director φ_1 entonces es superior al término director φ_{i+1} para $i = 1, 2, 3, \ldots$ sea $ax_1^{R_1}x_2^{R_2}\ldots x_m^{R_m}$ el término director de polinomio φ_1, φ_2 siendo simétrico, se deduce del lema 2.4 que $k_1 \geq k_2 \geq \ldots \geq k_m$. Sea $(l_1, l_2, \ldots, l_m)$ el vector de los índices del término director de un polinomio simétrico cualquiera φ_1 de la cadena (1) diferente de φ_1. En virtud de (1)

$$(k_1, k_2, \ldots k_m) > (l_1, l_2, \ldots, l_m),$$

por lo tanto,

(2) $k_1 \geq l_1 \geq l_2 \ldots l_m$.

Se constituye a esas condiciones, condiciones menos estrictas

(3) $0 \leq l_1 \leq, k_1, \ldots, 0 \leq l_m \leq k_1$.

El número de vectores $(l_1, \ldots, l_m)$ de N^m que satisface a las condiciones (3) para k_1 fijo es aparentemente finito y es $(k_1 + 1)^m$ .También el número de vectores $(l_1, \ldots, l_m)$ que satisface a la condición (2) es igualmente finito, ya que la condición (2) se deduce de la condición (3) , por lo consiguiente la cadena (3) no puede ser infinita. □

TEOREMA fundamental de los polinomios simétricos. Sea $\mathcal{K}\,[x_1,\ldots,x_m]$ un anillo de los polinomios en $x_1,\ldots,x_m$ sobre un dominio de integridad $\mathcal{K}$. Se $\sigma_1,\ldots,\sigma_m$ de los polinomios simétricos en $x_1,\ldots,x_m$. Todo polinomio $g\,(\sigma_1,\ldots,\sigma_m)$ sobre $\mathcal{K}$ se considerara como un polinomio simétrico

$g\left(\sigma_1(x_1,\ldots,x_m)\right),\ \ldots,\sigma_m(x_1,\ldots,x_m))$ En $x_1,\ldots,x_m$ sobre $\mathcal{K}$.

TEOREMA 2.7. *Todo polinomio simétrico del anillo de los polinomios* $\mathcal{K}\,[x_1,\ldots,x_m]$ *se puede representar bajo la forma de un polinomio sobre* $\mathcal{K}$ *compuesto de polinomios simétricos elementales* $\sigma_1,\ldots,\sigma_m$, *es decir que para todo* $f\,(x_1,\ldots,x_m) \in \mathcal{K}\,[x_1,\ldots,x_m]$ *existe un polinomio* $g(x_1,\ldots,x_m) \in \mathcal{K}\,[x_1,\ldots,x_m]$ *tal que*

$$f\,(x_1,\ldots,x_m) = g\left(\sigma_1(x_1,\ldots,x_m)\right),\ \ldots,\sigma_m(x_1,\ldots,x_m)).$$

Demostración. Sea f un polinomio simétrico no nulo sobre $\mathcal{K}$ y $a_0x_1^{R_1}\ldots x_m^{R_m}$ son término directo. El polinomio (1) $f_1 = f - a_0\sigma^{R1-R2}\ldots\sigma_m^{R_m}$ es simétrico dado que es una diferencia de polinomios simétricos además según el lema 2.5 $f > f_1$. Sea $a_1x_1^{l_1}\ldots x_m^{l_m}$ el término directo del polinomio f_1. De manera análoga,

(2) $f_2 = f - a_1\sigma^{l_1-l_2}\ldots\sigma_m^{l_m}$

es un polinomio simétrico con $f_1 > f_2$, etc. Se obtiene finalmente una cadena descendiente de polinomios simétricos $f_0 > f_1 > f_2 > \ldots$ Según el lema 2.6 esta cadena no puede ser infinita. Supóngase que sea para $(S + 1)$ ieme etapa, es decir

$$(s+1)f_{s+1} = f_s - a_s\sigma_1^{n_1-n_2}. \ . \ .\sigma_m^{l_m} = 0$$

Sumando término por términos las igualdades (1), (2), . . ., $(S+1)$, se obtiene

$$f = a_0\sigma^{R_1-R_2}. \ . \ .\sigma_m^{R_m} + a_1\sigma_1^{l_1-l_2} \ . \ . \ .\sigma_m^{l_m} + \ . \ . \ . + a_s\sigma_1^{n_1-nm_2}. \ . \ .\sigma_m^{n_m}$$

Esta igualdad proporciona la representación que se busca del polinomio simétrico f bajo la forma de un polinomio sobre $\mathcal{K}$ compuesto de polinomios simétricos elementales $\sigma_1,. \ . \ .\sigma_m$.□

Ejemplo. $x_1^2 + x_2^2 + . \ . \ . + x_m^2 = (x_1 + . \ . \ . + x_m)2 - (x_1x_2 + . \ . \ . + x_{m-1}x_m) = \sigma_1^2 - 2\sigma_2$.

COROLARIO 2.8. Sea $\varphi = z^m + a_1z^{m-1} + \cdots + a_m$ un polinomio sobre un anillo numérico $\mathcal{K}$ y $\varphi = (z-c_1)(z-c_2)\cdots(z-c_m)$, o $c_1, \cdots, c_m \in$ C. Si $f(x_1, \cdots, x_m)$ es un polinomio simétrico en $x_1, \cdots, x_m$ *con coeficientes en* K, *entonces* $f(c_1, \cdots, c_m) \in$ K.

Demostración. De la igualdad

$$(z-c_1)(z-c_2)\cdots(z-c_m) = z^m + a_1z^{m-1} + a_2z^{m-2} + \cdots + a_m$$

se deducen las fórmulas siguientes (Viète) que expresa la relación que vincula las raíces y los coeficientes del polinomio

$$c_1 + \cdots + c_m = -a_1;$$
$$c_1c_2 + \cdots + c_{m-1}c_m = a_2;$$
$$\cdots\cdots \ \cdots\cdots\cdots\cdots\cdots\cdots$$
$$c_1c_2\cdots c_m = (-1)^m a_{m.}$$

Estas igualdades pueden representarse bajo la forma

$$\sigma_1(c_1, \cdots, c_m) = -a_1;$$
$$\sigma_2(c_1, \cdots, c_m) = a_2;$$
(1) ……..
$$\sigma_m(c_1, \cdots, c_m) = (-1)^m a_m.$$

Conforme al TEOREMA fundamental de los polinomios simétricos, el polinomio $f \ de \ K\ [x_1, \cdots, x_m]$ se puede representar bajo la forma de un polinomio g compuesto de polinomios simétricos elementales $\sigma_1, \cdots, \sigma_m$ con coeficientes en K, es decir

(2) $f(x_1, \cdots, x_m) = g\big(\sigma_1(x_1, \cdots, x_m), \cdots, \sigma_m(x_1, \cdots, x_m)\big)$.

Al plantearse la igualdad (2) $x_1 = c_1, \cdots, x_m = c_m \ y$, dada la igualdad (1), se obtiene

(3) $f(c_1, \cdots, c_m) = g(-a_1, a_2, \cdots, (-1)^m a_m)$.

Además, $g \in K[x_1, \cdots, x_m]$ y $a_1, \cdots, a_m \ \in K$, por consiguiente, $f(c_1, \cdots, c_m) \ \in K$. □

Ejercicios

1. ¿El polinomio $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ se puede considerar como un polinomio simétrico?
2. Busque el término director de un polinomio $2\sigma_1^4\sigma_2^3\sigma_3^2$, donde $\sigma_1 = x_1 + x_2 + x_3, \ \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3, \sigma_3 = x_1x_2x_3$.

3. Mostrar que el conjunto de todos los polinomios simétricos de $K\ [x_1, \cdots, x_n]$, donde K es el conjunto base del dominio de integridad $\mathcal{K}$, se cierra en el anillo de polinomios $\mathcal{K}[x_1, \cdots, x_n]$.
4. Buscar la suma de los cubos de las raíces complejas del polinomio $2_{z^4} - 4_{z^3} + 2_{z^2} - 6_z + 1$.
5. Buscar la suma de los cuadrados de las raíces complejas del polinomio $x^n + a_{n-1^{x^{n-1}}} + \cdots + a_{1^x} + a_0$ sobre el cuerpo de números complejos.

§ 3. Resultados de polinomios y eliminación de variables

Resultado de dos polinomios. Sean f y g polinomios del anillo de polinomios $\mathcal{F}[x]$ sobre el cuerpo $\mathcal{F}$. Búsquese las condiciones por las cuales estos polinomios tienen un divisor común de potencia positiva.

TEOREMA 3.1. *Sean f y g polinomios en x sobre el cuerpo $\mathcal{F}$como*

$$f = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
$$g = b_0x^m + b_1x^{m-1} + \cdots + b_m,$$

el cual al menos uno de los coeficientes a_0, b_0 es diferente de cero. Los polinomios f y g tienen un divisor común de potencia positiva en $\mathcal{F}[x]$ si y solo si existe en $\mathcal{F}[x]$ los polinomios $c\ y\ d$ que satisface las condiciones:

$(\alpha)\ fc = gd,$
$(\beta)\ c = c_0x^{m-1} + \cdots + c_{m-1},$
$$d = d_0x^{n-1} + \cdots + d_{n-1},$$
(γ) *al menos uno de los polinomios $c\ y\ d$ es diferente de cero.*

DEMOSTRACIÓN. Supóngase que los polinomios f y g tienen en $\mathcal{F}[x]$ un divisor común u de potencia positiva. Existen entonces los polinomios $c\ y\ d$ como $f = du, g = cu$. Se verifica fácilmente que los polinomios $c\ y\ d$ satisfacen las condiciones $(\alpha) - (\gamma)$. Supóngase que hasta el momento existen polinomios c, d que satisfacen las condiciones $(\alpha), (\beta)\ y\ (\gamma)$. Plantéese que el grado del polinomio f equivale a n, es decir $a_0 \neq 0$ (en caso contrario se puede intervenir los roles de $f\ y\ g$). Sea φ el común divisor de $c\ y\ d$. Entonces en $\mathcal{F}[x]$ se encuentran los polinomios $c_1\ y\ d_1$ tal que

(1) $c = c_1\varphi, \qquad d = d_1\varphi, \qquad \text{MCD}(c_1, d_1) = 1.$

Nótese que $d_1 \neq 0$, ya que en el caso contrario $d = 0$ y a razón de $(\alpha), c = 0$, el cual está en contradicción con la condición (γ). Conforme a (1) y a la condición $(\alpha), fc_1\varphi = gd_1\varphi$ y como resultado,

(2) $fc_1 = gd_1.$

El polinomio d_1 que divide fc_1 y que es primo con c_1, d_1 divide a f; de modo que

(3) $f = d_1t,$

donde t es un polinomio de grado positivo, dado que el grado de d_1 no es superior al grado de d, asi como el grado de d es inferior al grado de f, conforme a la condición (β). De (3) y (2) se deduce $d_1th = gd_1\ y\ g = ht$. Por lo tanto, $f\ y\ g$ tienen un divisor común t de potencia positiva. □

Escríbase las condiciones $(\alpha)\ y\ (\beta)$ más detalladas:

(1) $(a_0x^n + \cdots + a_n)(c_0x^{m-1} + \cdots + c_{m-1}) = (b_0x^m + \cdots + b_m)(d_0x^{n-1} + \cdots + d_{n-1}).$

Después de efectuar la multiplicación de ambos términos de la igualdad e igualar los coeficientes de las mismas potencias de x, resulta un sistema que sigue las ecuaciones lineales

$$
\begin{aligned}
a_0c_0 &= b_0d_0;\\
a_1c_0 + a_0c_1 &= b_1d_0 + b_0d_1;\\
a_2c_0 + a_1c_1 + a_0c_2 &= b_2d_0 + b_1d_1 + b_0d_2;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
a_nc_{m-2} + a_{n-1}c_{m-1} &= b_md_{n-2} + b_{m-1}d_{n-1};\\
a_nc_{m-1} &= b_md_{n-1}.
\end{aligned}
$$

Este es un sistema de $n+m$ ecuaciones lineales homogéneas a $n+m$ variables $c_0, c_1, \cdots, c_{m-1}, d_0, d_1, \cdots, d_{n-1}$. Se tiene soluciones no nulas si y sólo si el determinante de ese sistema es nulo. Para evitar la aparición de menos antes los elementos de la matriz del determinante, se puede hacer pasar los segundos términos en el los primeros y considerar como variables $c_0, c_1, \cdots, c_{m-1}, -d_0, -d_1, \cdots, -d_{n-1}$. Si además se traspone la matriz del determinante, se obtiene la formula en este último

$$
R = \left|\begin{array}{cccccccccccc}
a_0 & a_1 & \ldots & a_n & & & & & & & & \\
 & a_0 & a_1 & \ldots & a_n & & & & & & & \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
 & & & & & & a_0 & a_1 & \ldots & a_n & & \\
b_0 & b_1 & & \ldots & b_m & & & & & & & \\
 & b_0 & b_1 & \ldots & & b_m & & & & & & \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
 & & & & & & b_0 & b_1 & \ldots & b_m & &
\end{array}\right| \begin{array}{l} \} m \\ \} n \end{array}
$$

DEFINICIÓN. Se le llama resultado de polinomios a $f = a_0x^n + \cdots + a_n$ y $g = b_0x^m + \cdots b_m$ el *determinante* R.

Se deduce del TEOREMA 3.1 que los polinomios $f\ y\ g\ (o\ a_0 \neq 0)\ o\ b_0 \neq 0$ aceptan un divisor común de potencia positiva si y sólo si el sistema de ecuaciones lineales tiene soluciones no nulas, es decir cuando el determinante R es nulo. En resumen, se demuestra el TEOREMA siguiente.

TEOREMA 3.2. *Sea* $f = a_0x^n + \cdots + a_n,\ g = b_0x^m + \cdots + b_m$ *polinomios sobre el cuerpo* $\mathcal{F}$ *y al menos uno de los coeficientes* $a_0 y\ b_0$ *no es nulo. Los polinomios* $f y\ g$ *tienen un divisor común de potencia positiva si y solo si el resultado de estos polinomios equivale cero.*

COROLARIO 3.3. Si el resultado de los polinomios $f\ y\ g$ es nulo, entonces los polinomios que tengan un divisor común de potencia positiva, o los coeficientes $a_0\ y\ b_0$ son nulos, y recíprocamente.

Eliminación de las variables. Se puede aplicar el resultado para eliminar variables del sistema de dos ecuaciones algebraicas, de las cuales al menos una no es lineal y tiene dos variables. Sea dado un sistema de ecuaciones

(1) $f(x,y) = 0, \qquad g(x,y) = 0,$

donde $f y\ g$ son polinomios en x y y sobre el cuerpo $\mathcal{F}$. Escríbanse estos polinomios seguidos de las potencias reducidas de x,

$$
\begin{aligned}
f\ (x,y) &= a_0\ (y)\ x^n + a_1\ (y)\ x^{n-1} + \cdots + a_n\ (y);\\
g\ (x,y) &= b_0\ (y)\ x^m + b_1\ (y)\ x^{m-1} + \cdots + b_n\ (y),
\end{aligned}
$$

donde $a_i\ (y)\ y\ b_k$ son polinomios del anillo $\mathcal{F}\ [y]$. Búsquese el resultado de los polinomios $f\ y\ g$ y considerándolos como los polinomios en x. Este resultado es un polinomio del anillo $\mathcal{F}[y]$ que se denotara $R\ (y)$.

Supóngase que el sistema (1) admite en el cuerpo $\mathcal{F}$ (o en su extensión) una solución (α, β). En ese caso los polinomios

$$f(x,\beta)\ =\ a_0\ (\beta)\ x^n\ +\ a_1\ (\beta)\ x^{n-1}\ +\cdots+\ a_n\ (\beta);$$
$$g\ (x,\beta)\ =\ b_0\ (\beta)\ x^m\ +\ b_1\ (\beta)\ x^{m-1}\ +\ \cdots+\ b_m\ (\beta)$$

tienen una misma raíz α. Así pues, los polinomios tienen un múltiplo común de potencia positiva $\left(sobre\ F(\beta)\right)$. Como resultado, conforme al TEOREMA 3.2, su resultado igual a R (β) debería ser igual a cero. Recíprocamente: si β es una raíz del resultado de $R\ (y)$, es decir R $(\beta) = 0$, entonces, según el corolario 3.3, lo polinomios $f(x,\beta)$ y $g(x,\beta)$ tienen una raíz común, dados sus coeficientes $a_0\ (\beta)$ y $b_0\ (\beta)$ son ambos nulos.

De este modo, la solución del sistema de ecuaciones (1) para dos variables se reduce a la solución de la ecuación

(2) $R(y) = 0$

en un variable y. Se dice que la ecuación (2) es el resultado de la eliminación de x del sistema de ecuaciones (1).

Ejemplo. Búsquese las soluciones del sistema de ecuaciones

$$x^2y^2\ +\ x^2y\ +y+x=0,$$
(1)
$$xy^2\ +2xy\ +1=0.$$

Elimínese x del sistema (1). Para hacer eso escríbase los primeros elementos de las ecuaciones seguidas de las potencias reducidas de x:

$$(y^2\ +y)\ x^2+x+y=0,$$
(2)
$$(y^2+2y)\ x+1=0$$

y fórmese el determinante:

$$R(y)=\begin{vmatrix} y^2+y & 1 & y \\ y^2+2y & 1 & 0 \\ 0 & y^2+2y & 1 \end{vmatrix}.$$

Al calcular el determinante, se obtiene

$$R(y)\ =\ y^2+y+y(y^2+2y)^2-y^2-2y=$$
$$=y\ [(y^2+2y)^2-1].$$

La ecuación $R\ (y) = y\ [(y^2+2y)^2-1] = y\ (y+1)^2\ (y^2+2y)-1$ propone raíces $0, -1, -1+\ \sqrt{2}, -1-\sqrt{2}.$

Para $y=-1$ el sistema (1) se transforma en un sistema $x-1=0, -x+1=0$. Así, se obtiene la solución del sistema (1): $(1,-1)$. Para $y=-1\pm\sqrt{2}$ el sistema (1) se transforma en sistema

$$\left(2\pm\sqrt{2}\right)x^2+x+\left(-1\pm\sqrt{2}\right)=0,$$
$$x+1=0,$$

cuya solución es $x=-1$. Como resultado, se obtiene dos soluciones del sistema (1):$\left(-1,-1+\sqrt{2}\right), \left(-1,-1-\sqrt{2}\right)$.

Ejercicios

1. Calcular el resultado de los polinomios:

(a) $2x^3 - 3x^2 + 2x + 1\ y\ x^2 + x + 3$;

(b) $x^3 + 2x^2 + 2x - 2\ y\ x^2 - 2x + 4$;

(c) $x^3 - 3x + 6\ y\ x^3 + x^2 - x - 1$.

2. Para cual valor de λ los polinomios tienen una raíz común:

(a) $x^3 - 2\lambda x + \lambda^3\ y\ x^2 + \lambda^2 - 2$;

(b) $x^3 + \lambda x^2 - 9\ y\ x^2 + \lambda x - 3$?

3. Eliminar x del sistema de ecuaciones

$x^2 - 3xy + y^2 - 2 = 0,\ \ 2x^2 - xy + 3y^2 - 1 = 0.$

4. Al utilizar el resultado resuelva el sistema de ecuaciones

$y^2 + x^2 - y - 3x = 0,\quad y^2 - 6xy - x^2 + 11y + 7y - 12 = 0.$

CAPITULO XVI

POLINOMIOS SOBRE UN CUERPO DE NÚMEROS COMPLEJOS Y SOBRE UN CUERPO DE NÚMEROS REALES

§ 1.Cuerpo de números complejos algebraicamente cerrado

TEOREMA del desarrollo del módulo de un polinomio. Sea $\mathcal{C}[z]$un anillo de polinomios sobre un cuerpo de números complejos $\mathcal{C}$ y $C[z]$ su conjunto de base.

TEOREMA 1.1. *Sea f un polinomio de grado positivo de $C[z]$. Para cualquier número real $M > 0$, existe un número real $r > 0$ al igual que para cualquier número complejo $z|f\ (z)| \geq M$, al igual que $|z| \geq r$.*

Demostración. Sea

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n \in C[z], \qquad a_n \neq 0, \quad n \geq 1.$$

Conforme a las propiedades del módulo (TEOREMA 4.7.8),

$$|a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0| \geq |a_n z^n| - |a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}|,$$
$$|a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}| \leq |a_0| + |a_1||z| + \cdots + |a_{n-1}||z|^{n-1}.$$

Como resultado, para $z \neq 0$

$$(1)\ \ |f(z)| \geq |a_n||z|^n \left[1 - \left(\frac{|a_0|}{|a_n||z|^n} + \cdots + \frac{|a_{n-1}|}{|a_n||z|}\right)\right].$$

Plantéese

$$(2)\ \ b = \max\left\{\frac{|a_0|}{|a_n|}, \ldots, \frac{|a_{n-1}|}{|a_n|}\right\}.$$

Nótese que para $k \geq 1$ y $z \geq 1$ las desigualdades $|z|^k \geq |z|$ y

(3) $\frac{1}{|z|^k} \leq \frac{1}{|z|}$

se cumplen. Sobre la base de (1)-(3), se deduce

(4) $|f(z)| \geq |a_n||z|^n \left(1 - \frac{nb}{|z|}\right)$.

Se deduce fácilmente que

(5) $\left(1 - \frac{nb}{|z|}\right) \geq \frac{1}{2}$ si $|z| \geq 2nb$.

A continuación, se tiene

(6) $\frac{|a_n||z|^n}{2} \geq M,$ si $|z| \geq \left(\frac{2M}{|a_n|}\right)^{1/n}$.

Sobre la base (4)-(6), se concluye que

$|f(z)| \geq M,$ si $|z| \geq r,$

donde $r = \max\left\{1, 2nb, \left(\frac{2M}{|a_n|}\right)^{1/n}\right\}$. □

Continuidad del módulo de un polinomio. Sea f un polinomio en z sobre el cuerpo de numero complejos. La aplicación $z \to |f(z)|$ se define sobre el conjunto C de todos los números complejos es una función real de la variable compleja. Se le denominará *módulo del polinomio* f y se le designara el símbolo $|f|$.

TEOREMA 1.2. Sea f un polinomio cualquiera de $C[z]$. El módulo del polinomio f es una función continua sobre el conjunto C.

Demostración. Muéstrese que para todo ε positivo existe un δ positivo que para cualquier número complejo z si $|z - a| < \delta$, entonces $\|f(z)| - |f(a)\| < \varepsilon$.

El TEOREMA es aparentemente verdadero si el polinomio f es nulo o de grado 0. Supóngase que el polinomio f es de grado n positivo.

Despéjese f como potencias de la diferencia $z - a$:

$$f(z) = c_0 + c_1(z - a) + \cdots + c_n(z - a)^n \quad (c_n \neq 0).$$

Como $f(a) = c_0$, se obtiene

$$f(z) - f(a) = c_1(z - a) + \cdots + c_n(z - a)^n$$

y, según el TEOREMA 4.7.8 se deduce la desigualdad

(1) $|f(z) - f(a)| \leq |c_1||z - a| + \cdots + |c_n||z - a|^n$.

Plantéese

$$b = max\{|c_1|, \ldots, |c_n|\};$$

Como $c_n \neq 0, b \neq 0$. Se deduce sin duda que para $k \geq 1$, se obtiene

(2) $|z-a|^k \leq |z-a|$ si $|z-a| \leq 1$.

Conforme a (1) y (2), se tiene

$$|f(z) - f(a)| \leq nb|z-a|.$$

Así mismo, para cualquiera $\varepsilon > 0$

$nb|z-a| < \varepsilon, si\ |z-a| < \varepsilon/nb.$

Asóciese a cada número ε un δ positivo así que $\delta = min\left\{\frac{\varepsilon}{nb}, 1\right\}$; entonces $|f(z) - f(a)| < \varepsilon$ si $|z-a| < \delta$. Así mismo, para cualquier número complejo z

$$\|f(z)| - |f(a)\| \leq |f(z) - f(a)|.$$

Por consiguiente, para cualquier $\varepsilon > 0$ existe $\delta > 0$ asi que para todo z de C, se obtenga

$\|f(z)| - |f(a)\| < \varepsilon$ si $|z-a| < \delta$. □

TEOREMA 1.3. *Sea f un polinomio de $C[z]$. Si la serie $\langle z_n \rangle$ converge hacia un número complejo a, entonces la serie $\langle |f(z_n)| \rangle$ converge hacia el número $|f(a)|$.*

Demostración. Según el TEOREMA 1.2,

(1) $(\forall \varepsilon > 0)(\exists \delta > 0)(\forall z \in C)(|z-a| < \delta \rightarrow \|f(z)| - |f(a)\| < \varepsilon)$.

Por hipótesis, la serie $\langle z_n \rangle$ converge hacia el número a. Así pues, para cualquier $\delta > 0$ existe un número natural $n_0$como $|z_n - a| < \delta$ con $n > n_0$ cualquiera. De ahí, conforme a (1), se deduce

$$(\forall \varepsilon > 0)(\exists n_0 \in \mathrm{N})(\forall n \in \mathrm{N})(n > n_0 \rightarrow \|f(z_n)| - |f(a)\| < \varepsilon).$$

Así, la serie $\langle |f(z_n)| \rangle$ converge hacia el número $|f(a)|$. □

Valor mínimo del módulo de un polinomio. Para presentar lo anterior, se necesitará del famoso TEOREMA del análisis de Bolzano-Weierstrass: de cualquier serie infinita $\langle z_n \rangle$ de los puntos del círculo $|z| \leq r$ (r sea un número real positivo fijo) se puede extraer una sub-serie que converge en un cierto punto del círculo.

TEOREMA 1.4. *Sea f un polinomio de $C[z], r$ un número real positivo y $m = \inf_{|z| \geq r} |f(z)|$. Entonces, existe un número complejo a tal que $|f(a)| = m\ y\ |a| \leq r$.*

Demostración. Sea $\langle \varepsilon_n \rangle$ una serie de números reales positivos que convergen hacia 0. Como $m = \inf_{|z| \geq r} |f(z)|$, existe para cada término ε_n de la serie un z_n que verifica

(1) $m \leq |f(z_n)| \leq m + \varepsilon_n, \quad |z_n| \leq r.$

(2)

También la serie $|f(z_n)|$ converge hacia m:

(3) $\lim_{n\to\infty} |f\ (z_n)| = m.$

Conforme a (1), todos los elementos de la serie $\langle z_n \rangle$ pertenecen al círculo $|z| \leq r$. Según el TEOREMA de Bolzano-Weierstrass esta serie genera una sub-serie $\langle x_n \rangle$ que converge en un cierto punto a del círculo $|z| \leq r$, es decir

(4) $\lim_{n\to\infty} x_n = a, \quad |a| \leq r.$

Según el TEOREMA 1.3, de (3) se deduce

(5) $\lim_{n\to\infty} |f(x_n)| = |f(a)|.$

Dado que $\langle |f(x_n)| \rangle$ es una sub-serie $\langle f\ (z_n) \rangle$ que converge hacia m, se tiene

(6) $\lim_{n\to\infty} |f(x_n)| = m.$

Sobre la base (3), (4) y (5) se concluye que $|f(a)| = m$ y $|a| \leq r$. □

TEOREMA 1.5. *Un módulo de polinomio cualquiera f de $C[z]$ tiene su valor mínimo sobre el conjunto C.*

Demostración. El TEOREMA es al parecer verdadero si $\text{grad } f = 0$ o $f(0) = 0$. Supóngase entonces que $\text{grad } f \geq 1$ y $f(0) \neq 0$.

Plantéese $M = |f(0)|$. Según el TEOREMA 1.1, se tiene

(1) $(\exists r > 0)(\forall z \in C)(|z| \geq r \rightarrow |f(z)| \geq M).$

Sea $K = \{z \in C \| z| \leq r\}$. Según el TEOREMA 1.4, $|f|$ admite el menor valor en el círculo K, es decir que existe un número a asi como

(2) $|f(a)| \leq |f(z)|$ si $|z| \leq r$, en particular,

(3) $|f(a)| \leq |f(0)| = M.$

Sobre la base de (1) y (3), se concluye que

(4) $|f(a)| \leq |f(z)|$ si $|z| \geq r.$

Conforme a (2) y (4), se obtiene $(\forall z \in C)\ (|f(a)| \leq |f(z)|)$. Así mismo, $|f|$afecta sobre el conjunto C el valor mínimo al punto a.□

Lema de D'Alembert. La demostración del TEOREMA 1.7 se basa en gran parte en el lema siguiente llamado lema de D'Alembert.

LEMA 1.6. Sea $f(x)$ un polinomio de grado positivo sobre el cuerpo de números complejos y $a \in C$. Si $f(a) \neq 0$, existe un número complejo c tal como $|f(c)| < |f(a)|$.

Demostración. Sea $f(x) = a_0 + \cdots + a_n x^n$ un polinomio de grado $n > 0$ y $f(a) \neq 0$. Despéjese f en potencias de la diferencia $x - a$:

(1) $f(x) = c_0 + c_1(x-a) + \cdots + c_n(x-a)^n, donde\ c_i \in C, c_0 = f(a) \neq 0, c_n \neq 0.$

Plantéese $z = x - a$ y

(2) $g(z) = c_0 + c_1 z + \cdots + c_n z^n$.

Sea c_m un coeficiente no nulo de un polinomio g a un índice menor positivo $(0 < m \leq n)$; entonces

(3) $f(a+z) = g(z) = c_0 + c_m z^m + c_{m+1} z^{m+1} + \cdots + c_n z^n$.

(4)

Defínase $h(z)$:

(5) $h(z) = \begin{cases} c_{m+1} + \cdots + c_n z^{n-m-1} \; si \; m > n, \\ 0 \quad si \quad m = n. \end{cases}$

Entonces la igualdad (3) puede escribirse bajo la forma

(6) $g(z) = c_0 + c_m z^m + z^{m+1} h(z)$.

Conforme a (1), $\frac{c_0}{c_m} \neq 0$. Nótese d una raíz m- ésima cualquiera del número $(-c_0/c_m)^{c_m}$:

(7) $d^m = -c_0/c_m$.

Considérese (5) el valor de z bajo la forma

(8) $z = \lambda d$, donde $0 < \lambda < 1, \quad \lambda \in R$.

Conforme a (5) y (6), se obtienen las igualdades

(9) $\begin{matrix} g(\lambda d) = c_0 - c_0 \lambda^m + \lambda^{m+1} d^{m+1} h(\lambda d), \\ g(\lambda d) = c_0 [1 - \lambda^m + \lambda^{m+1} c_0^{-1} d^{m+1} h(\lambda d)]. \end{matrix}$

En la base de (4), se concluye que

$d^{m+1} h(\lambda d) = c_{m+1} d^{m+1} + \cdots + c_n d^n \lambda^{n-m-1} \quad (m < n);$

y $\left| c_0^{-1} d^{m+1} h(\lambda d) \right| \leq |c_0|^{-1} [|c_{m+1} d^{m+1}| + \cdots + |c_n d^n|] \quad (m < n).$

Plantéese ahora

(10) $B = \begin{cases} c_0|^{-1} [|c_{m+1} d^{m+1}| + \cdots + |c_n d^n|] \; si \; m < n, \\ 0 \quad si \quad m = n \end{cases}$

Nótese que para $m < n, B > 0$, dado que $c_n \; y \; d$ son diferentes de cero.

De (8) y (9) se deduce la desigualdad

$|g(\lambda d)| \leq |c_0| [1 - \lambda^m + \lambda^{m+1} B] = |c_0| [1 - \lambda^m (1 - \lambda B)].$

Si λ satisface las condiciones $0 < \lambda < 1, \lambda B < 1, |g(\lambda d)| < |c_0|$.

como $c_0 = f(a)$ y, conforme a (3), $g(\lambda d) = f(a + \lambda d)$, entonces se tiene

$|f(a + \lambda d)| < |f(a)|$ si $\begin{cases} 0 < \lambda < min\{1, B^{-1}\} \; para \; m < n, \\ 0 < \lambda < 1 \; con \; m = n. \end{cases}$ □

Clausura algebraica de un cuerpo de números complejos. Sea $\mathcal{F}[x]$ un anillo de polinomios en x sobre el cuerpo $\mathcal{F}$.

DEFINICIÓN. Un cuerpo $\mathcal{F}$ es *algebraicamente cerrado* si todos los polinomios de grado positivo $\mathcal{F}[x]$ poseen en el cuerpo $\mathcal{F}$ al menos una raíz.

TEOREMA 1.7. *Un cuerpo de números complejos es algebraicamente cerrado*.

Demostración. Sea f un polinomio cualquiera de grado positivo de $\mathcal{F}[x]$. Si $f = (0) = 0$, entonces el cero es una raíz del polinomio f. Admítase que $f(0) \neq 0$ y plantéese $M = |f(0)|$. Sea r un número positivo por el cual

(1) $(\forall z \in C)(|z| \geq r \rightarrow M \leq |f(z)|)$.

Este número positivo r existe conforme al TEOREMA 1.1.

Sea $K = \{z \in C \big| |z| \leq r\}$. Conforme al TEOREMA 1.4, la función $|f|$ tiene el valor mínimo sobre el conjunto K, es decir que existe un número $a \in K$, así que

(2) $|f(a)| \leq |f(z)|$ para todo $z \in K(|z| \leq r)$

y en particular,

(3) $|f(a)| \leq |f(0)| = M$.

De (1) y (3), se obtiene

(4) $(\forall z \in C)(|z| \geq r_0 \rightarrow |f(a)| \leq |f(z)|)$.

Sobre la base de (2) y (4), se concluye que

(5) $(\forall z \in C)(|f(a)| \leq f|(z)|)$.

Si $f(a) \neq 0$, entonces, según el lema de D'Alembert, existe un numero complejo a tal que

$|f(c)| < |f(a)| \qquad (c \in C)$.

Ahora bien, esta última desigualdad es opuesta a (5), por eso el en caso de $f(a) \neq 0$ es imposible. Como resultado $f(a) = 0$, es decir el número complejo a es una raíz del polinomio f. □

COROLARIO. 1.8. *Cualquier polinomio del anillo $\mathcal{C}[x]$, en el cual el grado es superior a la unidad, es reducible en el anillo $\mathcal{C}[x]$.*

Demostración. Sean $f \in \mathcal{C}[x]$ y $\operatorname{grad} f > 1$. Según el TEOREMA 1.7, existe un $a \in C$ semejante a $f(a) = 0$. Entonces, según el TEOREMA 14.1.11, $(x - a)$ divide f, es decir que existe un polinomio g en $\mathcal{C}[x]$, semejante a $f = (x - a) \cdot g$. Además, $\operatorname{grad} g > 0$, dado que $\operatorname{grad} f > 1$. Así, el polinomio f es irreducible en el anillo $\mathcal{C}[x]$.

COROLARIO 1.9. *Cualquier polinomio f de grado positivo del anillo $\mathcal{C}[x]$ puede representarse de manera única bajo la forma del producto de un número complejo y de los factores lineales repetidos, es decir bajo la forma*

(1) $f = c(x - \alpha_1) \cdots (x - \alpha_n)$,

donde $\alpha_1, \cdots, \alpha_n$ son raíces del polinomio f (en C) y c el coeficiente dominante del polinomio.

Esta afirmación se deriva del corolario 1.8 y del TEOREMA 14.2.11 de la descomposición del polinomio sobre el cuerpo de un producto de los factores normados irreducibles.

Si en la descomposición (1) $\alpha_1, \cdots, \alpha_m$ todas las raíces son distintas al polinomio f en C, entonces esta descomposición puede representarse bajo la forma

(2) $f = c(x - \propto_1)^{k_m}, k_1 + \cdots + k_m = n.$

La descomposición (2) se llama *descomposición canónica del polinomio f en factores irreducibles*. El número k_s se llama *índice de multiplicidad de la raíz α_s*.

COROLARIO 1.10. *Todo polinomio f de grado positivo n de $C[x]$ admite exactamente n raíces complejas si se cuenta cada raíz tantas veces lo que vale su multiplicidad.*

Formula de Viète. Establézcase la relación entre las raíces y los coeficientes de un polinomio.

TEOREMA 1.11. Sean $f = z^n + c_1 z^{n-1} + \cdots + c_{n-1} z + c_n$ un polinomio sobre el cuerpo de números complejos y $\alpha_1, \cdots, \alpha_n$ sus raíces; entonces

$$
\begin{aligned}
& c_1 = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n); \\
& c_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n; \\
& c_3 = -(\alpha_1\alpha_2\alpha_3 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n); \\
& \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& c_n = (-1)^n \alpha_1\alpha_2 \cdots \alpha_n.
\end{aligned} \tag{1}
$$

Demostración. Dado que $\alpha_1, \cdots, \alpha_n$ son raíces del polinomio f, según el corolario 1.9, se deduce

$$z^n + c_1 z^{n-1} + \cdots + c_{n-1} z + c_n = (z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n).$$

Al multiplicar los factores lineales en el segundo término de la igualdad, se obtiene

$$z^n + c_1 z^{n-1} + \cdots + c_{n-1} z + c_n = z^n - (\alpha_1 + \cdots + \alpha_n) z^{n-1} + \cdots + (-1)^n \alpha_1\alpha_2 \cdots \alpha_n.$$

De la igualdad de dos polinomios en z se deduce una igualdad de coeficientes de las mismas potencias de z; igualando los coeficientes de las mismas potencias de z, se obtienen las fórmulas (1). □

Las fórmulas (1) se llaman *fórmulas de Viète*.

COROLARIO 1.12. Si $\alpha_1, \cdots, \alpha_n$ son las raíces de un polinomio $c_0 z^n + c_1 z^{n-1} + \cdots + c_{n-1} z + c_n$ de grado n de $C[z]$, entonces

$$
\begin{aligned}
& \frac{c_1}{c_0} = -(\alpha_1 + \cdots + \alpha_n); \\
& \frac{c_2}{c_0} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n; \\
& \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& \frac{c_n}{c_0} = (-1)^n \alpha_1\alpha_2 \cdots \alpha_n.
\end{aligned}
$$

Ejercicios

1. Descomponer en factores lineales en el anillo $\mathcal{C}[z]$ los polinomios:

(a) $z^2 + z + 1 + i$; (b) $z^4 + z^3 - z - 1$.

2. Descomponer en factores irreducibles el polinomio $z^4 + 3z^3 + 4z^2 + 3z + 1$ en el anillo $\mathcal{C}[z]$ y en $\mathcal{R}[z]$.
3. Descomponer el polinomio $z^n - 1$, donde n es un numero natural diferente de cero y de 1, en factores lineales de $\mathcal{C}[z]$.
4. La suma de dos raíces de la ecuación $2x^3 - x^2 - 7x + \lambda = 0$ es igual a 1. Buscar λ.
5. Determinar λ de manera que una de las raíces de la ecuación $x^3 - 7x + \lambda = 0$ sea igual o el doble que la otra.
6. Al saber que el polinomio $z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$, donde $+ a_{n-1}, \ldots, a_0$ son números complejos y tienen las raíces $\alpha_1, \cdots, \alpha_n$, calcular el producto $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1)$.
7. Sea $b^2 < 4ac$, donde a, b, c, son números reales. Demostrar que el anillo cociente $\mathcal{R}[z]/(az^2 + bz + c)$ es isomorfo en el cuerpo de números complejos.
8. Demostrar la proposición inversa del TEOREMA de Viète (fórmulas (1)), entonces los números complejos $\alpha_1, \cdots, \alpha_n$ son las raíces del polinomio $f = z^n + c_1 z^{n-1} + \ldots + c_n$ sobre el cuerpo $\mathcal{C}$.

§2. Polinomios sobre un cuerpo de números reales

Conjugación de raíces imaginarias de un polinomio con coeficientes reales. Sea $\mathcal{R}[x]$ un anillo de polinomios sobre el cuerpo $\mathcal{R}$ de números reales.

Recuérdese que un número complejo $a + bi$, donde $a, b \in R$, se dice imaginario si $b \neq 0$. Si $\alpha = a + bi$, se notará $\bar{\alpha}$ el número complejo conjugado $a - bi$.

LEMA 2.1. *Si f es un polinomio del anillo $\mathcal{R}[x]$ y α un número complejo cualquiera, entonces $f(\bar{\alpha}) = \overline{f(\alpha)}$.*

La demostración se deriva directamente del TEOREMA 4.7.6.

TEOREMA 2.2. *Sea f un polinomio cualquiera del anillo $\mathcal{R}[x]$. Si $a + bi$ es una raíz imaginaria del polinomio f, $a - bi$ es igual a una raíz de ese polinomio.*

Demostración. Sea $a + bi$ una raíz del polinomio, es decir $f(a + bi) = 0$. Entonces, según el lema 2.1, $f(a - bi) = f\overline{(a + bi)} = \overline{f(a + bi)} = \bar{0} = 0$, es decir $f(a - bi) = 0$. □

Polinomios irreducibles sobre el cuerpo de número reales.

TEOREMA 2.3. *Sea f un polinomio cuyo grado es superior a la unidad, irreducible sobre un cuerpo $\mathcal{R}$ de números reales. Existe entonces de $a, b \in R$ tales que $b \neq 0$ y el polinomio f se asocia al polinomio $(x - a)^2 + b^2$.*

Demostración. Según el TEOREMA 1.7, el polinomio f admite al menos una raíz compleja. Sea $a + bi$ una raíz del polinomio f, donde $a, b \in R$. Si $b = 0$, entonces $x - a$ divide f sobre $\mathcal{R}$. Como resultado, $b \neq 0$. Aplíquese a los polinomios f y $(x - a)^2 + b$ el TEOREMA de la división con residuo. Según este TEOREMA, existe en el anillo $\mathcal{R}[x]$ los polinomios $q(x)$ y $cx + d$ tal que

$$f(x) = q(x)[(x - a)^2 + b^2] + (cx + d), \quad c, d \in R.$$

Al plantear en esta igualdad $x = a + bi$, se obtiene

$$f(a + bi) = c(a + bi) + d = 0, (ca + d) + bci = 0.$$

Se deduce que $ca + d = 0, bc = 0$. Ahora bien, $b \neq 0$, por tanto $c = 0$ y $d = 0$. Así,

$$f(x)[(x - a)^2 + b^2].$$

Puesto que, por hipótesis, el polinomio f es irreducible sobre $\mathcal{R}$, el grado del polinomio $q(x)$ equivale a cero. Como resultado, el polinomio f se asocia al polinomio $(x - a)^2 + b^2$.□

COROLARIO 2.4. *En el anillo $\mathcal{R}[x]$ no son reducibles más que los polinomios del primer grado, así mismo que los polinomios del segundo grado asociados a los polinomios de la forma $(x-a)^2+b^2$, donde a y b son números reales cualquieras y $b \neq 0$.*

Del corolario 2.4 y del TEOREMA 14.2.11 se deriva el TEOREMA siguiente.

TEOREMA 2.5. *Cualquier polinomio f de grado positivo del anillo $\mathcal{R}[x]$ se puede representar de manera única baja la forma de un producto de un número real y de los polinomios de 2-esimo grado más irreducibles sobre $\mathcal{R}$:*

$f = d\prod_k\left[(x-a_k)^2 + b_k^2\right]\prod_s(x-c_s)$, donde $b_k \neq 0$.

COROLARIO 2.6. *Cualquier polinomio con coeficientes reales admite un número par de raíces imaginarias.*

COROLARIO 2.7. *Un polinomio de grado impar con coeficientes reales admite al menos una raíz real.*

COROLARIO 2.8. *Sea f un polinomio de grado n de $\mathcal{R}[x]$. La paridad del número de raíces reales del polinomio f coincide con las del número n.*

Ejercicios

1. Buscar el polinomio de los coeficientes reales y de grados mínimos que admiten las raíces $i-1, \pi, -1+\sqrt{3}$.
2. Descomponer en factores irreductibles en la estructura delos números reales los polinomios.
   (a) x^3+x+2; $(b)\ x^4+2x^2+4$; $(c)x^5-1$; $(d)\ x^4-x^2+1$.
3. Descomponer el polinomio x^4+4 en factores irreductibles: (a) en la estructura $\mathcal{C}$; (b) en la estructura $\mathcal{R}$; (c) en la estructura $\mathcal{Q}$.
4. Descomponer en factores irreductibles en la estructura de los números reales el polinomio $x^4-ax^2+1, donde -2<a<2$.
5. Demostrar que el polinomio $x^{3m}+x^{3n+1}+x^{3p+2}$ es divisible por el polinomio x^2+x+1.
6. Sea f un polinomio en la estructura de los números reales cuyo coeficiente dominante y el término libre son signos opuestos. Demostrar que el polinomio f admite al menos una raíz real.

§ 3. Ecuación de tercer y cuarto grado

Ecuación de tercer grado. La ecuación

(1) $x^3+px+q=0 \qquad (p,q \in \mathbf{C})$

se denomina *ecuación cubica incompleta.* Plantéese en la ecuación (1) $x=u+v$, es decir, en lugar de una variable introdúzcase dos.

Se obtiene,

$$(u+v)^3+p(u+v)+q=0,$$

ó

(2) $u^3+v^3+q+(3uv+p)(u+v)=0.$

Exíjase que se cumpla la condición $3uv+p=0$, dicho de otra manera, la condición $uv=-p/3$. Al cumplirse esta condición, $u\ y\ v$ confirma el sistema

$$u^3+v^3=-q, \qquad uv=-p/3.$$

En la base de (3), (2) y (1), se concluye: si (u,v) es la solución del sistema (3) la suma $u+v$ es la solución de la ecuación (1).

Muéstrese que la proposición inversa es igualmente verdadera: si x es la raíz de la ecuación (1), existe una solución (u, v) del sistema (3), tal que $x = u + v$. En efecto, sea x la raíz de la ecuación (1).
Considérese la ecuación

$$y^2 - xy - p/3 = 0.$$

Sean u, v sus raíces complejas. Entonces, al aplicarse las fórmulas de Viète, se obtiene

$$x = u + v, \qquad uv = -p/3$$

x siendo la raíz de la ecuación (1), (u, v) es por lo tanto la solución de (2) y, por consiguiente, la solución (3). Así mismo, conociendo la solución del sistema (3) se puede obtener todas las raíces de la ecuación (1).

El sistema de ecuaciones

(3) $u^3 + v^3 = -q, \qquad u^3 v^3 = -p^3/27,$

se implica aparentemente por el sistema (3). Los números u, v cumplen con (4) si y sólo si u^3, v^3 son las raíces de la ecuación cuadrática

(4) $z^2 + qz - p^3/27 = 0.$

Esta ecuación se llama *reducción por ecuación (1).* Su discriminante se designa por Δ .

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

Las raíces z_1, z_2 de la ecuación (5) se expresan por las fórmulas

(5) $z_1 = u^3 = -q/2 + \sqrt{\Delta}, \qquad z_2 = v^3 = -q/2 - \sqrt{\Delta}.$

(6)

De ésta se obtienen nueve soluciones del sistema (4). Al seleccionar por medio de estas últimas soluciones (u, v) del sistema (4) el cual cumple con la condición $uv = -p/3$, se obtienen todas las soluciones del sistema (3).

El sistema (3) admite una solución al menos. En efecto, sea (u_1, v_1) cualquiera de las soluciones del sistema (4), entonces $u_1^3, v_1^3 = -p^3/27$.
Como resultado,

$$u_1 v_1 = -\frac{p}{3}, \text{ ó } u_1 v_1 = -\frac{p}{3}.\varepsilon, \quad \text{ó } u_1 v_1 = -\frac{p}{3}.\varepsilon^2, donde\ \varepsilon^3 = 1;$$

Entonces

$$u_1 v_1 = -\frac{p}{3}, \text{ ó } v_1(v_1 \varepsilon^3) = -\frac{p}{3}, \text{ ó } u_1(v_1 \varepsilon) = -\frac{P}{3}.$$

Por consecuencia, para cualquier valor u de la raíz cubica de z_2, tal que $uv = -p/3$, es decir, que el par (u, v) será una solución del sistema (3).

Si $u, u\varepsilon, u\varepsilon^2$ son los valores de la raíz cúbica de z_1, le corresponde $v, v_\varepsilon, v\varepsilon$, valores de la raíz cúbica de v_2. Así que, si (u, v)es una solución cualquiera del sistema (3), entonces $(u, v), (u\varepsilon, v\varepsilon^2), (u\varepsilon^2, v\varepsilon)$ es la colección de cualquier solución del sistema (3) el cual admite tres soluciones diferentes. Se concluye entonces que la ecuación (1) admite las soluciones siguientes:

(7) $x_1 = u + v, \qquad x_2 = u\varepsilon + v\varepsilon^2, \qquad x_3 = v\varepsilon^2 + v\varepsilon.$

TEOREMA 3.1. Sea dada la ecuación

(1) $x^3 + px + q = 0.$

Sean z_1 y z_2 las raíces de la ecuación resolviente $z^2 + qz - p^3/27 = 0.$
Las raíces de la ecuación (1) se expresan por las fórmulas

(I) $X_1 = u + v, \quad x_2 = u\varepsilon + v\varepsilon^2 \quad x_3 = u\varepsilon^2 + v\varepsilon$

donde u y v son números que cumplen con las condiciones

(*) $u^3 = z_1, \quad v^3 = u_2, \quad uv = -p/3.$

y ε es la raíz cubica imaginaria de la unidad.

Demostración. Una verificación directa muestra que $x^3 + px + q$ es divisible entre $x - x_1$, el cociente siendo igual a $x^2 + x_1x + x_1^2 + p$; como resultado,

(2) $x^3 + px + q = (x - x_1)(x^3 + x_1x + x_1^2 + p).$

Luego, se tiene que

(3) $(x - x_2)(x - x_3) = x^3 - (x_2 + x_3)x + x_2x_3.$

En virtud de las fórmulas de Viète

(4) $1 + \varepsilon + \varepsilon^2 = 0\ y\ \varepsilon + \varepsilon^2 = -1.$

De esta y de las fórmulas (I), se deduce que

(5) $x_1 + x_2 + x_3 = 0, \quad -(x_2 + x_3) = x_1.$

En virtud de las fórmulas (I), (*) y (4), se obtiene

$$x_2x_3 = (u\varepsilon + v\varepsilon^2)(u\varepsilon^2 + u\varepsilon) = u^2 + v^2 + uv(\varepsilon^2 + \varepsilon) =$$
$$= u^2 + v^2 - uv = (u + v)^2 + 3uv = x_1^2 + p,$$

Es decir

(6) $x_2x_3 = x_1^2 + p.$

En virtud de (5) y (6), la fórmula (3) puede escribirse bajo la forma

(7) $(x - x_2)(x - x_3) = x^3 + x_1x + x_1^2 + p.$

Basándose en (2) y (7), se concluye que

$x^3 + px + q = (x - x_1)(x - x_2)(x - x_3).$ □

COROLARIO 3.2. Las raíces de la ecuación (1) se expresan por las fórmulas

(II) $x_1 = u + v; \qquad x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v);$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v),$$

donde $u\ y\ v$ son números que cumplen con las condiciones (*).

Demostración. Las fórmulas (II) se obtienen a partir de las fórmulas (I) si se plantea $\varepsilon = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. □

Estudio de las raíces de la ecuación de tercer grado con coeficientes reales. El TEOREMA siguiente permite determinar el número de raíces reales e imaginarias de una ecuación de tercer grado.

TEOREMA 3.3. *Sean*

(1) $x^3 + px + q = 0$

una ecuación de coeficientes reales y $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$. *Entonces:*

(a) Si $\Delta > 0, la\ ecuación\ (1)\ admite\ una\ raíz\ real\ y\ dos\ imaginarias\ conjugadas$;

(b) $si\ \Delta = 0, las\ raices\ de\ la\ ecuación\ (1)\ son\ reales\ y\ una\ de\ ellas\ al\ menos\ es\ multiple.$

(c) $si\ \Delta < 0, cualquier\ raíz\ de\ la\ ecuación\ (1)\ es\ real\ y\ distinta.$

Demostración. Primer caso: $\Delta > 0$. En este caso las raíces $z_1\ y\ z_2$ de la ecuación resolvente son reales y distintas. Como resultado, una de ellas al menos, por ejemplo, z_1, es diferente a cero. Sea $u = (z_1)^{1/3}$ la raíz aritmética de z_1. El número u es igualmente un número real, dado que $uv = p/3$. Dado que $z_1 \neq z_2$ y por consecuencia, $u^3 \neq v^3$, se tiene $u \neq v$. Según el corolario 3.2,

(II) $x_1 = u + v, \qquad x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u+v),$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v)$$

u y v siendo números reales distintos, se deducen las fórmulas (II) que x_1 es una raíz real, dado que $x_2\ y\ x_3$ son imaginarias conjugadas.

Segundo caso: $\Delta = 0. Si\ \Delta = 0\ y\ q \neq 0, z_1 = z_2 = -q/2 \neq 0. Sea\ u = (-q/2)^{1/3}$ una raíz aritmética del número $-q/2\,. uv = p/3$ siendo un número real, da como resultado $u = (-q/2)^{1/3}, es\ decir, u = v \neq 0$. En virtud de las fórmulas (II), se deduce:

$$x_1 = 2u \neq 0, \qquad x_2 = x_3 = -u.$$

Así mismo, con $q \neq 0$ la ecuación (I) admite tres raíces reales de las cuales una es doble.

Pero si $\Delta = 0\ y\ q = 0, entonces\ p = 0$. En este caso la ecuación (I) toma la forma $x^3 = 0$. Como resultado, $x_1 = x_2 = x_3 = 0$.

Tercer caso: $\Delta < 0$. $En\ este\ caso\ z_1 = -q/2 + \sqrt{\Delta},\ z_2 = -q/2 - \sqrt{\Delta}$.

Como resultado, $z_1\ y\ z_2$ son números imaginarios conjugados y, por consiguiente,

(1) $|z_1| = |z_2| \neq 0$

y

(2) $z_1 \neq z_2$.

En virtud del TEOREMA 3.1, existen números $u\ y\ v$ tales que

(3) $u^3 = z_1, \qquad uv = -p/3, \qquad v^3 = z_2.$

Se deduce de (1) y (3) que $|u|^3 = |v|^2 \neq 0\ y$, como resultado,

(4) $|u| = |v| \neq 0.$

En virtud de (2),

(5) $u \neq v.$

En la base de (3) y (4), se concluye que

(6) $-\frac{p}{3|u|^2} = 1.$

En la base de (3) y (6), se obtiene

(7) $v = -\frac{p}{3u} = -\frac{p}{3u\bar{u}} \cdot \bar{u} = -\frac{p}{3|u|^2} \cdot \bar{u} = \bar{u}.$

Se deduce de (5) y (7) que $u\ y\ v$ son números imaginarios conjugados. Según el corolario 3.2, se obtiene:

$$x_1 = u + v;$$

(III) $$x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v);$$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v)$$

Como $\bar{u} = v\ y\ u \neq v$, se deduce de estas fórmulas que cualquiera de las raíces $x_1, x_2\ y\ x_3$ es reales. Además, estas son de dos en dos diferentes. De hecho, en virtud de las fórmulas (II), $x_2 \neq x_3$. Supóngase que $x_1 = x_2$. Entonces, en virtud de las fórmulas (I), $u + v = u\varepsilon + v\varepsilon^2, de\ donde\ u(1-\varepsilon) = v(\varepsilon^2 - 1); entonces, u = v\varepsilon^2. de\ ahi\ igualmente\ se\ obtiene\ z_1 = z_2\ y\ \Delta = 0$; sin embargo esta última igualdad está en contradicción con la condición $\Delta < 0$.

De manera análoga se prueba que $x_1 \neq x_3$. □

Ecuación de cuarto grado. El método de Ferrari permite resolver la ecuación del cuarto grado reduciendo la operación de la resolución de una ecuación auxiliar del tercer grado. El principio del método de Ferrari es el siguiente. La ecuación dada del cuarto grado con coeficientes complejos

(1) $x^4 + ax^3 + bx^2 + cx + d = 0$

se escribe bajo la forma de $x^4 + ax^3 = -bx^2 - cx - d$. Al agregar a los dos miembros de la ecuación $a^2\,x^2/4$, como resultado

$$(x^2 + \frac{ax}{2})^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d.$$

Luego, al agregar a los dos miembros de la ecuación la suma

$$\left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4},$$

Se obtienen en el primer miembro de la ecuación un cuadrado perfecto:

(2) $(x^2+\frac{ax}{2}+\frac{y}{2})^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\frac{y^2}{4}-d.$

El trinomio derecho está en función del parámetro y. Selecciónese este parámetro y de manera que el trinomio sea un cuadrado de un binomio de primer grado en x. Para que el trinomio Ax^2+Bx+C sea un cuadrado del binomio en x, basta que $B^2-4AC=0$. De hecho, al cumplir con esta condición, se obtiene

$$Ax^2+Bx+C=Ax^2+2\sqrt{\overline{AC}}\,x+C=(2\sqrt{\overline{Ax}}+\sqrt{\overline{C}})^2.$$

Es necesario entonces seleccionar y en el segundo número de (2) de manera que se cumpla la condición

$$(\frac{ay}{2}-c)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0,$$

El cual se puede escribir bajo la forma

(3) $y^3-by^2+(ac-4d)y-[c^2+d(a^2-4b)]=0.$

Al cumplirse esta condición, el segundo miembro d la ecuación (2) será un cuadrado de un binomio lineal en x.

Al resolver la ecuación auxiliar (3), se obtiene una de sus raíces y_0. Luego, búsquese los números $m\ y\ n$ volviendo el cuadrado del binomio $mx+n$ igual al segundo número de la igualdad (2), entonces

(4) $x^2+\frac{ax}{2}+\frac{y_0}{2})^2=(mx+n)^2,$

donde $m=\sqrt{\overline{\frac{a^2}{4}-b+y_0}},\qquad n=\sqrt{\overline{\frac{y_0^2}{4}-d}}.$ La resolución de la ecuación (4) se reduce a la resolución del sistema de dos ecuaciones cuadráticas siguientes:

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=mx+n,\qquad x^2+\frac{ax}{2}+\frac{y_0}{2}=-mx-n.$$

Una vez resueltas las dos ecuaciones, se obtienen cuatro raíces de la ecuación de partida (1).

Ejercicios

1. Resuelva las siguientes ecuaciones de tercer grado:

(a) $x^3-3x+2=0;$ $(b)\ x^3-6x+4=0;$

(c)$x^3+3x-x+4=0;$ $(d)\ x^3+3x-2i=0.$

(2). Resuelva las siguientes ecuaciones de cuarto grado:

(a) $x^4+2x^3+2x^2+x-7=0;$

(b) $x^4-x^3-x^2+2x-2=0;$

(c) $x^4+12+3=0.$

3. demostrar que $(x_1-x_2)^2(x_1-x_3)^2(x_1-x_3)^2=-4p^3--27q^2, donde\ x_1,x_2,x_3$ son las raíces de la ecuación $x^3+px+q=0.$

§ 4. Separación de raíces reales de un polinomio

Sistema de polinomios de Sturm. Sea f un polinomio de coeficientes reales, siendo $a\ y\ b, a<b$ números reales cuales quiera no constituyentes de las raíces del polinomio.

Más adelante, al recurrir al método de Sturm, se resuelve el problema que consiste en encontrar el número exacto de raíces reales distintas del polinomio f en el intervalo $a < x < b$.

Supóngase dada la serie final de números reales, por ejemplo, 2,5,-3,4,-5,-2,7. Los signos de números de esta serie alternan de la manera siguiente: $+, +, -, +, -, -, +$ y varían cuatro veces. Así mismo, en esta serie se tiene cuatro variaciones de signos.

Sea f un polinomio de grados positivo con coeficientes reales y desprovisto de raíces reales múltiples. Defínase la serie final de polinomios $f_0, f_1, f_2 \dots f_m$ en la base de un polinomio dado $f_0 = f$, de la manera siguiente:

$f_1 = f', donde\ f'\ es\ la\ derivada\ de\ f;$
$f_0 = q_1 f_1 - f_2;$
$f_1 = q_2 f_2 - f_3;$
……
$f_{m-1} = q_m f_m.$

También se aplicó en los polinomios $f\ y\ f'$ el algoritmo de Euclide) (método de divisiones sucesivas) atribuyendo a cada variación del resto un signo opuesto.

DEFINICIÓN. La serie de los polinomios $f_0, f_1, f_2 \dots f_m$ se llama *sistema de polinomios f de Sturm.*

Nótese cualquier propiedad de polinomios del sistema de Sturm.

PROPIEDAD 4.1.Cada dos polinomios próximos del sistema de Sturm se disminuyen de raíces reales comunes.

Demostración. Esta afirmación es verdadera para los polinomios $f_0\ y\ f_1(f, f_1 = f')$, dado que f no tiene raíces reales múltiples. Tres polinomios que se siguen se ligan por la igualdad

$(^*)\ f_{\kappa-1} = q_\kappa f_\kappa - f_{\kappa+1}.$

En virtud de esta igualdad la anulación simultánea de dos polinomios vecinos $f_\kappa\ y\ f_{\kappa-1}$ arrastraría la anulación simultánea de $f_{\kappa-1}\ y\ f_\kappa$, seguido, de los polinomios $f_{\kappa-2}\ y\ f_{\kappa-1}$, entre otras, y por último los polinomios $f_0\ y\ f_1$, lo cual es imposible. □

PROPIEDAD 4.2. *Si y es una raíz real de un polinomio intermedio $f_\kappa, 1 \le \kappa < m$, entonces los números $f_{\kappa-1}(\gamma)\ y\ f_{\kappa+1}\ (\gamma)$ son signos diferentes.*

Demostración. En efecto, si $f_\kappa\ (\gamma) = 0$, entonces al plantearse en la igualdad $(^*)\ x = \gamma,\ se\ obtiene\ f_{\kappa-1}(\gamma) = -f_{\kappa+1}(\gamma)$. □

TEOREMA de Sturm. Para demostrar el TEOREMA de Sturm se utilizará el siguiente TEOREMA de Weierstrass: si una función real f continúa en el intervalo $[a, b]$ y los números $f(a), f(b)$ son de signos opuestos, entonces f admite una raíz entre $a\ y\ b$.

Sea f un polinomio de coeficientes reales. Supóngase que por cada número real $c, w\ (c)$ designa el número de variaciones de signos en la serie numérica $f_0(c), f_1(c), \dots, f_m(c)$ en la cual se omiten todos los ceros.

TEOREMA (DE STURM). *Sean f un polinomio de coeficientes reales que no posee raíces reales múltiples y*

(1) $f_1, f_1, \dots, f_m$

el sistema de polinomios f de Sturm. Sean $a\ y\ b\ (a < b)$ números reales cuales quieras los cuales no son raíces del polinomio f. El número de raíces reales distintas del polinomio f en el intervalo (a, b) es igual a la diferencia $w\ (a) - w\ (b)$.

Demostración. Sea M el conjunto de cualquier raíz real de polinomios (1). Los elementos del conjunto M dividen el intervalo (a, b) en sub-intervalo. En cada uno de estos sub-intervalos ningún polinomio (1) se anula. En virtud del TEOREMA de Weierstrass, se deduce que en cada sub-intervalo cualquier polinomio (1) conserva su signo y, por

consiguiente, el número $w(c)$ pasando por el valor real γ por el cual se anula al menos uno de los polinomios (1), es decir $\gamma \in M$.

Sean $\alpha\ y\ \beta\ (\alpha < \beta)$ puntos interiores de dos sub-intervalos vecinos adyacentes en el punto γ. Demostremos que la diferencia $w\ (\alpha) - w(\beta)$ se expresan por las fórmulas

(2) $\mathrm{w}\,(\alpha) - \mathrm{w}(\beta) = \begin{cases} 1 \text{ si } \mathrm{f}(\gamma) = 0, \\ 0 \text{ si } \mathrm{f}(\gamma) \neq 0. \end{cases}$

Admítase que γ es la raíz del polinomio f_κ, donde $1 \leq \kappa < \mathrm{m}$. Según la propiedad 4.2, los números $\mathrm{f}_{\kappa-1}(\gamma)$ y $\mathrm{f}_{\kappa+1}(\gamma)$ poseen signos opuestos. Entonces, en dos sub-intervalos adyacentes en γ y los valores de los polinomios $\mathrm{f}_{\kappa-1}$ y $\mathrm{f}_{\kappa+1}$ se asignan signos opuestos.

Como resultado, el número de variaciones de signos en las series

$$\mathrm{f}_{\kappa-1}(\alpha), \mathrm{f}_\kappa(\alpha), \mathrm{f}_{\kappa+1}(\alpha)\ \text{y}\ \mathrm{f}_{\kappa-1}(\alpha), \mathrm{f}_\kappa(\beta), \mathrm{f}_{\kappa+1}(\beta)$$

es el mismo, a saber es igual a la unidad. En las otras partes del sistema de polinomios (1) el número de variaciones de signos sigue estacionario. Como resultado, en el caso considerado $\mathrm{w}(\alpha) - \mathrm{w}(\beta) = 0$.

Ahora supóngase que γ es la raíz del polinomio $\mathrm{f}(\ \mathrm{f} = \mathrm{f}_0, \mathrm{f}_1 = \mathrm{f}')$. Dado que, por hipótesis, el polinomio f es desprovisto de las raíces reales múltiples, existe un polinomio g de coeficientes reales, tales que

(3) $\mathrm{f}_0(\mathrm{x}) = (\mathrm{x} - \mathrm{y})\mathrm{g}\,(\mathrm{x}), \qquad \mathrm{g}(\gamma) \neq 0.$

Como resultado,

(4) $\mathrm{f}_1(\mathrm{x}) = \mathrm{g}(\mathrm{x}) + (\mathrm{x} - \gamma)\mathrm{g}'\,(\mathrm{x}).$

En virtud de (4) el signo del polinomio f_1 en el punto γ y, como resultado, en los dos sub-intervalos adyacentes en γ coincide con el del número $\mathrm{g}(\gamma)$. Sin embargo, en virtud de (3), el signo de f_0 para cada valor de x coincide con el de $(\mathrm{x} - \gamma)\ \mathrm{g}\ (\gamma)$. Entonces, entre $\mathrm{f}_0(\alpha)$ y $\mathrm{f}_1(\alpha)$ no tiene una variación de signos, en cuanto a los números $\mathrm{f}_0(\beta)$ y $\mathrm{f}_1(\beta)$, se asignan del mismo signo. Además, todas las variaciones posibles de signos en la serie (1), como ya se mostró, se mantiene con el paso por el signo γ. Así mismo, en el caso considerado tenemos $\mathrm{w}\ (\alpha) - \mathrm{w}\ (\beta) = 1$.

En resumen, se demostró que es solamente con el paso por el valor de la raíz del polinomio f que el número $\mathrm{w}\ (\mathrm{c})$ disminuye de una unidad. Como resultado, el número de raíces reales distintas del polinomio f es igual a la diferencia $\mathrm{w}\ (\mathrm{a}) - \mathrm{w}\ (\mathrm{b})$. □

El TEOREMA de Sturm se verifica igualmente en el caso donde el polinomio admite las raíces reales múltiples. La demostración del TEOREMA en este caso difiere poco de antes mencionada.

Para determinar el número todas las raíces reales distintas del polinomio f sirviéndose del TEOREMA de Sturm, es necesario escoger a y b de manera que ninguno de los polinomios del sistema de Sturm admita raíces exteriores del intervalo $\mathrm{a} \leq \mathrm{x} \leq \mathrm{b}$. en ese caso los signos de polinomios del sistema de Sturm se determinarán por los coeficientes dominantes. En efecto, para los grandes valores de x el signo del polinomio $\mathrm{a}_0\mathrm{x}^\mathrm{n} + \mathrm{a}_1\mathrm{x}^{\mathrm{n}-1} + \cdots + \mathrm{a}_\mathrm{n}$ coincide con el de a_0, mientras que para los grandes valores absolutos de valores negativos de x el signo del polinomio coincide con $(-1)^\mathrm{n}\mathrm{a}_0$. Por lo tanto no es necesario garantizar los valores suficientemente grandes en a y b, ya que basta con conocer los signos de los coeficientes dominantes de los polinomios f del sistema de Sturm, así mismo que los grados de estos polinomios.

Al utilizar el sistema de Sturm, se puede separar las raíces reales del polinomio f y, como resultado, encontrar los intervalos que no contienen ninguna raíz del polinomio f.

Ejemplo. Búsquese el número de raíces positivas y negativas del polinomio $\mathrm{f} = \mathrm{x}^4 - 4\mathrm{x}^2 + \mathrm{x} + 1$.

Al aplicar el método de divisiones sucesivas, se encuentra por f el siguiente sistema de polinomios de Sturm:

$\mathrm{f}_0 = \mathrm{f} = \mathrm{x}^4 - 4\mathrm{x}^2 + \mathrm{x} + 1;$

$\mathrm{f}_1 = 4\mathrm{x}^3 - 8\mathrm{x} + 1;$

$\mathrm{f}_2 = 8\mathrm{x}^2 - 3\mathrm{x} - 4;$

$\mathrm{f}_3 = 87\mathrm{x} - 28;$

$\mathrm{f}_4 = 1.$

Para un valor negativo y suficientemente grande en valor absoluto de x en la serie de signos será $+, -, +, -, +$ (cuatro variaciones de signos). Para $\mathrm{x} = 0$ los signos coinciden con los términos libres, es decir, $+, +, -, -, +$ (dos variaciones de signo).

Así mismo, se perdió dos variaciones de signos, entonces el polinomio f admite dos raíces negativas. Para un valor positivo suficientemente grande de x los signos de los términos dominantes son $+, +, +, +, +$ (cero variación de signos). Como resultado, el polinomio admite dos raíces positivas.

Ejercicios

1. Componer los polinomios de Sturm y separar las raíces de los polinomios:

(a) $x^3 - 3x - 3$; $(b)x^4 - x - 1$; $(c)x^4 - 4x^3 + 4x^2 - 4$; $(d)x^4 - 4x^2 - 1$.

2. Determinar con la ayudad del TEOREMA de Strum el número de raíces reales del polinomio $x^5 + px + q$ con coeficientes reales p y q.
3. Determine con la ayuda del TEOREMA de Sturm el número de raíces reales del polinomio $x^n + px + q \; con \; p \; y \; q$ reales.
4. Demostrar que si el sistema de Sturm por el polinomio f de grado n con coeficientes reales se compone de $n + 1$ polinomios, entonces el número de variaciones de signos en la serie de coeficientes dominantes de polinomios de Sturm es igual al número de pares de raíces complejas conjugadas del polinomio f.
5. Buscar el número de raíces reales del polinomio $x^4 - 2x^2 + 4x - 1$. ¿Entre que enteros sucesivos se disponen estas raíces?

CAPITULO XVII
POLINOMIOS EN UN CUERPO DE NÚMEROS RACIONALES Y NÚMEROS ALGEBRÁICOS
§1. Raíces enteras y racionales de un polinomio. Criterio de irreducibilidad

Raíces enteras y racionales de un polinomio. El TEOREMA siguiente nos permite encontrar las raíces racionales de un polinomio de coeficientes enteros.

TEOREMA 1.1. Sea m y q enteros primarios entre ellos y $q \neq 0$. Si m / q es una raíz del polinomio $a_0 + a_1 x + \cdots + a_n x^n$ de coeficientes enteros, entonces m divide $a_0 \; y \; q$ divide a_n

Demostración. Por hipótesis,

$$a_0 + a_1 \frac{m}{q} + \cdots + a_{n-1}(\frac{m}{q})^{n-1} + a_n \left(\frac{m}{q}\right)^n = 0.$$

Al multiplicar los dos números de la igualdad para q^n, se obtiene

(1) $a_0 q^n + a_1 m q^{n-1} + \cdots + a_{n-1} m^{n-1} + a_n m^n = 0.$

En la base de la igualdad (1) se concluye que m deivide $a_0 q^n$. Sin embargo, como los números $m\ y\ q$ son primeros entre ellos, los números $m\ y\ q^n$ también lo son. Entonces, m divide a_0.

En virtud de (1), q divide $a_n m^n$. Además, los números $q\ y\ m^m$ son primeros entre ellos porque por la hipótesis, los números $q\ y\ m$ son primeros entre ellos. Como resultado, q divide a_n.□

COROLARIO 1.2. *Si un entero m es una raíz del polinomio* $a_0 + a_1 x + \cdots x^n$ *con los coeficientes enteros es un número entero.*

COROLARIO 1.3 *Una raíz racional de un polinomio ordenado* $a_0 + a_1 x + \cdots + x^n$ *con coeficientes enteros es un número entero.*

Criterio de irreducibilidad de Eisenstein. El problema de reducibilidad de un polinomio en el anillo $Q[x]$ se reduce a su reducibilidad en el anillo $Z[x]$.

PROPOCIÓN 1.4. *Sea* f *un polinomio del anillo delos polinomios* $Z[x]$. *Si el polinomio* f *es reducible en el anillo* $Q[x]$ *es entonces reducible en el anillo* $Z[x]$.

Ya que el cuerpo Q es un cuerpo de cocientes del anillo Z de enteros, la proposición 1.4 deriva directamente del lema 14.3.5.

TEOREMA 1.5. *(CRITERIO DE EISENSTEIN). Sea* $f = c_0 + c_1 x + \cdots + c_n x^n$ *un polinomio con coeficientes enteros. Supóngase que cualquier coeficiente del polinomio* f *exceptuando el coeficiente dominante se divide por un número* primario p cualquiera, mientras que el término libre c_0 no se divide por p^2. Entonces el polinomio f es reducible en el anillo $Q[x]$.

Demostración. Supóngase que el polinomio f es reducible en el anillo $Q[x]$. Entonces, en virtud de la proposición 1.4, se reduce en el anillo $Z[x]$, es decir existe en Z $[x]$ de polinomios g y h de grados positivos tales que $f = gh$. Sea

$$g = a_0 + \cdots + a_k x^k,\ \ h = b_0 + \cdots + b_m x^m$$
$$(a_k \neq 0, \quad b_m \neq 0);$$

Entonces

(1) $f = \left(a_0 + \cdots + a_k x^k\right)(b_0 + \cdots + b_m x^m) =$
$$= c_0 + c_1 x + \cdots + c_n x^n,$$

Con $1 \leq k, m < n$,

(2) $c_0 = a_0 b_0$,
(3) $c_n = a_k b_m$.

Por hipótesis,

(4) $p | c_0, \qquad p^2 \nmid c_0$.

En virtud de (2) y (4), un solo de los números $a_0\ y\ b_0$ es divisible por p; sea

(5) $p | a_0, \qquad p \nmid b_0$.

Por hipótesis, $p \nmid c_0$. De ahí, en virtud de (3), se deduce que

(6) $p \nmid a_k$.

Supóngase que a_s el cual no es divisible por p es un coeficiente del polinomio g cuyo índice es el más pequeño, es decir

(7) $(p|a_0, \dots, p|a_{s-1}, \qquad p \nmid a_s \qquad (1 \le s \le k \le n).$

En virtud de (1), el coeficiente c_s puede representarse bajo la forma

$$c_s = a_s b_0 + (a_{s-1} + \cdots + a_0 b_s) \qquad (s < n).$$

Se deduce de (7) que p divide $a_{s-1}b_1 + \cdots + a_0 b_s$, y como p no divide $b_0\ y\ a_s, p\ no\ divide\ c_s, con\ s \le k < n$. Se contradice con la hipótesis del TEOREMA ya que este último, p divide los coeficientes $c_0, c_1, \dots, c_{n-1}$.□

CORALARIO 1.6. *Si p es primario y n es un entero positivo cualquiera, entonces el polinomio $x^n - p$ es reducible en el anillo $Q[x]$.*

Ejercicios

1. Demostrar que el polinomio f con coeficientes enteros no admiten raíces enteras si $f(0)\ y\ f(1)$ son números impares.
2. Establecer cuáles de los polinomios siguientes son irreducibles en el cuerpo de números racionales:
   $(a)2x^5 + 6x^4 - 9x^2 + 12; \quad (b)\ x^2 + x + 1;$
   $(c)x^2 + 3x - 4; \quad (d)x^3 - 12:\ (e)\ x^3 + x - 2;$
   $(F)x^3 - 3x + 5; \quad (g)x^4 - 2x + 3.$
3. Demostrar que el polinomio $\frac{xp-1}{x-1} = xp^{-1} + xp^{-2} + \cdots + x + 1,\ donde\ p$ es primario, es reducible en el cuerpo de números racionales.
4. Demostrar que el polinomio $x^3 - p,\ donde\ p$ es primario, es irreducible en el cuerpo de números racionales.
5. ¿Para cual entero n el polinomio $x^3 + n$ es reducible en la estructura de números racionales?
6. ¿Para qué entero $m\ y\ n$ el polinomio $m^3 + n$ es reducible en la estructura de número racionales?
7. Descomponer los polinomios $x^6 - 1$ y $x^8 - 1$ en factores irreducibles en la estructura de números racionales.
8. Encontrar las condiciones de reducibilidad del polinomio $x^4 + ax^2 + \beta$, dende α, β son números racionales, en la estructura de números racionales.
9. Demostrar que si el polinomio f es irreducible en la estructura Q de números racionales, entonces el polinomio $f(\alpha x + \beta), donde\ \alpha, \beta$ son números racionales y $\alpha \neq 0$, es igualmente irreducible en la estructura Q.

§ 2. Extensión algebraica simple de una estructura

Extensión algébrica simple de una estructura. Sea $\wp[\boldsymbol{x}]$ un anillo de polinomios en x en la estructura $\wp$**,** donde $\wp$ es un sub-cuerpo del cuerpo F**.** Recuérdese que el elemento $\alpha\ del\ cuerpo\ F$ se llama *algebraica de* $\wp$ si α es una raíz de un polinomio cualquiera de grados positivos de $\wp[\boldsymbol{x}]$.

DEFINICIÓN. Sean $\wp$ y $\alpha \in F$. Se llama *extensión simple de la estructura* $\wp$ *por adjunción del elemento* α el más pequeño sub-cuerpo del cuerpo F que contiene el elemento P y el elemento α. La extensión simple $\wp$ por adjunción de α se escribe $\wp(\boldsymbol{\alpha})$, en cuanto a el conjunto de base del cuerpo $\wp(\alpha)$, se escribe P(α).

Sean $\alpha \in F$, $\wp[x]$ un anillo de polinomios en x y

$$P[\alpha] = \{f(\alpha) | f \in P[x]\},$$

es decir $P[\alpha]$ es un conjunto de cualquier expresión de la forma $a_0 + a_1\alpha + \cdots + a_n\alpha^n, donde\ \ a_0, a_1, \dots, a_n \in P$ y n un número natural cualquiera.

Se constata que el algebra $\langle P[\alpha], +, -, ., 1\rangle$, sub-anillo del cuerpo $\wp(\boldsymbol{\alpha})$,es un anillo; es anillo se designa por el símbolo $\wp[\alpha]$.

TEOREMA 2.1. *Sean* $\mathcal{P}[\propto]$ *un anillo de los polinomios en* x *sobre* $\mathcal{P}$ *y* $\mathcal{P}(\alpha)$ *una extensión simple del cuerpo* $\mathcal{P}$. *Sea* φ *una aplicación de* $P[x]$ *sobre* $\mathcal{P}[\alpha]$*tal que*$\varphi(f) = f(\alpha)$ *para todo* f *de* $P[x]$. *Entonces*:

a) *para todo* a *de* $P\varphi(a) = a$;
b) $\varphi(x) = \alpha$;
c) φ*es un homomorfismo del anillo* $\mathcal{P}[x]$ *sobre el anillo* $\mathcal{P}[\alpha]$;
d) $Ker\ \varphi = \{f \in P[x] \mid f(\alpha) = 0\}$;
e) *El anillo cociente* $\mathcal{P}[x]/\ Ker\ \varphi$ *es isomorfo en el anillo* $\mathcal{P}[\alpha]$.

Demostración. Las afirmaciones (a) y (b) resultan directamente de las afirmaciones de la definición de φ. La afirmación φ respeta las operaciones principales del anillo $\mathcal{P}[x]$, puesto que para todos f y g de $P[x]$, se tiene

$$\varphi(f + g) = f(\alpha) + g(\alpha),\ \varphi(fg) = f(\alpha)\,g(\alpha),\ \varphi(1) = 1.$$

Luego, por hipótesis, φ es una aplicación de $P[x]$ sobre $P[\alpha]$. Por consiguiente, φ es un homomorfismo del anillo $\mathcal{P}[x]$ sobre el anillo $\mathcal{P}[\alpha]$.

La afirmación (d) se deriva directamente de la definición de la aplicación φ.

Puesto que φ es un homomorfismo del anillo $\mathcal{P}[x]$ sobre $\mathcal{P}[\alpha]$, según el TEOREMA 13.1.6, el anillo cociente $\mathcal{P}[x]/\ Ker\ \varphi$ es isomorfo al anillo $\mathcal{P}[\alpha]$. □

COROLARIO 2.2. *Sea* α *un elemento trascendente sobre el cuerpo* $\mathcal{P}$. *Entonces el anillo de polinomio*$\mathcal{P}[x]$ *es isomorfo en el anillo* $\mathcal{P}[\alpha]$.

Demostración. En virtud de la trascendencia de α sobre $\mathcal{P}$, $Ker\ \varphi = \{0\}$. Por lo tanto, según el TEOREMA 13.1.6, $\mathcal{P}[x]/\{0\} \cong \mathcal{P}[\alpha]$. Además el anillo cociente del anillo $\mathcal{P}[x]$ según el ideal nulo es isomorfo a $\mathcal{P}[x]$. Por consiguiente, $\mathcal{P}[x] \cong \mathcal{P}[\alpha]$.□

Polinomio mínimo del elemento algebraico. Sea $\mathcal{P}[x]$ un anillo de los polinomios sobre el cuerpo $\mathcal{P}$.

DEFINICIÓN. Sea α un elemento algebraico sobre el cuerpo $\mathcal{P}$. Se llama *polinomio mínimo del elemento* α *sobre el cuerpo* $\mathcal{P}$ al polinomio mónico de $\mathcal{P}[x]$ de grado mínimo que admite como raíz a α. El grado del polinomio mínimo se denomina*grado del elemento* α *sobre el cuerpo* $\mathcal{P}$.

Se ve fácilmente que para todo elemento α algebraico sobre $\mathcal{P}$ existe un polinomio mínimo.

PROPOSICIÓN 2.3. Si α es un elemento algebraico sobre el cuerpo $\mathcal{P}$ y g y φ sus polinomios mínimos sobre $\mathcal{P}$, entonces $g = \varphi$.

Demostración. Los grados de los polinomios mínimos g y φ coinciden. Si $g \neq \varphi$, el elemento α (de grado n sobre $\mathcal{P}$) es la raíz del polinomio $g - \varphi$, cuyo grado es inferior al del polinomio φ (inferior a n), lo que es imposible. Por consiguiente**,** $g = \varphi$.□

TEOREMA 2.4. *Sean* α *un elemento algebraico de grado* n *sobre el cuerpo* $\mathcal{P}(\alpha \notin P)$ *y* g *son polinomios mínimos sobre* $\mathcal{P}$. *Entonces:*

a) *El polinomio* g *es irreducible en el anillo* $\mathcal{P}[x]$;
b) *Si* $f(\alpha) = 0$, *donde* $f \in P[x]$, *entonces* g *divide a* f;
c) *El anillo cociente* $\mathcal{P}[x]/(g)$ *es isomorfo al anillo* $\mathcal{P}[\alpha]$;
d) $\mathcal{P}[x]/(g)$ *es un cuerpo;*
e) *El anillo* $\mathcal{P}[\alpha]$ *coincide con el cuerpo* $\mathcal{P}(\alpha)$.

Demostración. Supóngase que el polinomio g es reducible en el anillo $\mathcal{P}[x]$, es decir existe en $P[x]$polinomios φ y h tales que

$g = \varphi h, \qquad 1 \leqslant \operatorname{grad} \varphi, \qquad \operatorname{grad} h < \operatorname{grad} g = n$

En este caso, $g(\alpha) = \varphi(\alpha)h(\alpha) = 0.\mathcal{P}\ (\alpha)$siendo un cuerpo, $\varphi(\alpha) = 0$ o $h(\alpha) = 0$, lo que es imposible, dado que por hipótesis, el grado del elemento α sobre $\mathcal{P}$ vale n.

Supóngase que $f \in P\ [x]$ y $f(\alpha) = 0$. Por hipótesis $g(\alpha) = 0$.

Por lo tanto, f y g no pueden ser primos entre ellos. El polinomio g siendo irreducible, divide, por consiguiente af.

Sea φ un homomorfismo del anillo $\mathcal{P}\ [x]$ sobre el anillo $\mathcal{P}\ [\alpha](\varphi\ (f)\ = f\ (\alpha)$ para todo f de $P\ [x]$, considerado en el TEOREMA 2.1. En virtud de (b), el núcleo del homomorfismo φ está compuesto de los polinomios múltiplos de g, es decir $Ker\ \varphi\ = (g)$. Por consiguiente, según el TEOREMA 13.1.6, el anillo cociente $\mathcal{P} = \mathcal{P}\ [x]/(g)$es isomorfo al anillo $\mathcal{P}\ [\alpha]$.

Ya que $P\ [\alpha] \subset \mathcal{P}\ (\alpha),\ \ \mathcal{P}\ [\alpha]$ es un dominio de integridad. Como $\overline{\mathcal{P}} \cong \mathcal{P}\ [\alpha]$, el anillo cociente $\overline{\mathcal{P}}$ es igualmente un dominio de integridad. Se debe mostrar que todo elemento $\overline{f}$ no nulo de $\overline{\mathcal{P}}$ es inversible en $\overline{\mathcal{P}}$. Sea f un elemento de la clase según un sub-grupo $\overline{f}$. Como $\overline{f}\ = \overline{0}$, $f(\alpha)\ \neq 0$ igualmente; así pues el polinomio g no divide el polinomio f. El polinomio g siendo irreducible, resulta de los polinomios f y $g$que son primos entre ellos. Por consiguiente, existe en $P\ [x]$ polinomios u y v tales que$uf\ + vg\ = 1$. Se deduce la igualdad $\overline{uf}\ =\ \overline{1}$ mostrando que el elemento $\overline{f}$ es inversible en el anillo $\overline{\mathcal{P}}$. En resumen,se establece que el anillo cociente $\overline{\mathcal{P}}$ es un cuerpo.

En virtud de (c) y $(d)\mathcal{P}\ [\alpha]$ es un cuerpo y, como consecuencia, $P\ (\alpha)\ \subset\ P\ [\alpha]$., es evidente que $P\ [\alpha]\ \subset\ P\ (\alpha)$. Como consecuencia, $P\ [\alpha]\ =\ P\ (\alpha)$. Por consiguiente, el anillo $\mathcal{P}\ [\alpha]$ coincide con el cuerpo $\mathcal{P}\ (\alpha)$. □

Estructura de la extensión algebraica simple de un cuerpo.

TEOREMA 2.5. *Sea α un elemento algebraico de grado positivo n sobre el cuerpo $\mathcal{P}$. Entonces todo elemento del cuerpo $\mathcal{P}\ (\alpha)$ puede representarse de manera única bajo la forma de combinación lineal de n elementos 1, $\alpha, \ldots, \alpha^{n-1}$ con coeficientes en P.*

Demostración. Sea β un elemento cualquiera del cuerpo $\mathcal{P}\ (\alpha)$. Según el TEOREMA 2.4, $P\ (\alpha)\ =\ P\ [\alpha]$; existe pues en $P\ [x]$ un polinomio f tal que

(1) $\beta\ =\ f\ (\alpha)$.

Sea g un polinomio mínimo para α sobre $\mathcal{P}$; en virtud de las condiciones del TEOREMA, su grado vale n. Según el TEOREMA de la división con residuo, existe en $P\ [x]$polinomios h y r tales como

(2) $f\ =\ gh\ + r$, donde $r\ = 0$ o $\operatorname{grad} r\ <\operatorname{grad} g\ = n$, es decir $r\ =\ c_0\ +\ c_1 x + \ldots + c_{n-1}x^{n-1}(c_i\ \in P)$.

Al apoyarse en $(2)x\ =\ \alpha$ y, teniendo en cuenta que la igualdad (1), se obtiene

(3) $\beta\ =\ c_0\ +\ c_1\alpha + \ .\ .\ .\ + c_{n-1}\alpha^{n-1}$.

Muéstrese que el elemento β se representa de manera única bajo la forma de una combinación lineal delos elementos*1, $\alpha, \ldots, \alpha^{n-1}$*. Sea

(4) $\beta\ =\ d_0\ +\ d_1\ \alpha + \ .\ .\ .\ + d_{n-1}\alpha^{n-1}$ $\qquad\qquad (d_i\ \in P)$

cualquiera de estas representaciones. Considérese el polinomio φ

$\varphi\ = (c_0\ -\ d_0)\ + (c_1\ -\ d_1)\ x + \ .\ .\ .\ + (\ c_{n-1}\ -\ d_{n-1})\ x^{n-1}$.

El caso donde el grado de φ es inferior an es imposible. Así pues en virtud de (3) y (4), $\varphi\ (\alpha)\ =\ 0$ y el grado de φ es inferior al de g. Sólo es posible en el caso donde $\varphi\ = 0$, es decir $c_0\ = d_0\ , \ldots, c_{n-1}\ = d_{n-1}$. Por consiguiente, el elemento β se representa de manera única bajo la forma de una combinación lineal delos elementos*1, $\alpha, \ldots, \alpha^{n-1}$*.□

Eliminación de la irracionalidad algebraica en el denominador de una fracción. El problema de la eliminación de la irracionalidad algebraica en el denominador de una fracción es el siguiente. Sea α un elemento algebraico de grado $n > 1$ sobre el cuerpo $\mathcal{P}$; f y h son polinomios del anillo de los polinomios $\mathcal{P}[x]$ y $h(\alpha) \neq 0$. Se trata de representar el elemento $\frac{f(\alpha)}{h(\alpha)} \in P(\alpha)$bajo la forma de una combinación lineal de potencias del elemento α, es decir bajo la forma de $\varphi(\alpha)$, donde $\varphi \in P[x]$.

Este problema se resuelve de la siguiente manera. Sea g el polinomio minimo para α sobre $\mathcal{P}$. Dado que, según el TEOREMA 2.4, el polinomio es irreducible sobre $\mathcal{P}$ y $h(\alpha) \neq 0$, g no divide a h y, como consecuencia, los polinomios h y g son primos entre ellos. Existe pues en $P[x]$ polinomios u y v tales que

(1) $uh + vg = 1$.

Ya que $g(\alpha) = 0$, de (1) se deduce

$u(\alpha)\, h(\alpha) = 1$, $\qquad \frac{1}{h(\alpha)} = u(\alpha)$.

Por consiguiente, $f(\alpha) / h(\alpha) = f(\alpha)\, u(\alpha)$, con $f, u \in P[X]$ y $f(\alpha)u(\alpha) \in P[\alpha]$. En resumen, se eliminar la irracionalidad en el denominador de la fracción $\frac{f(\alpha)}{h(\alpha)}$.

Ejercicios

1. Buscar el polinomio mínimo para α sobre el cuerpo $\mathcal{P}$ si:
   (a) $\alpha = -i, \mathcal{P} = \mathcal{R}$; (b) $\alpha = i\sqrt{2}, \mathcal{P} = \mathcal{C}$;
   c) $\alpha = i\sqrt{2}; \mathcal{P} = \mathcal{Q}$; (d) $\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \mathcal{P} = \mathcal{Q}$;
   e) $\alpha = \sqrt[4]{2}, \quad \mathcal{P} = \mathcal{Q}$.

2. **Eliminar** la irracionalidad algebraica en el denominador de la fracción
$\frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}-1}$.

3. **Eliminar** la irracionalidad en el denominador de la fracción
$\frac{1}{\sqrt{2}+2\sqrt[4]{2}-1}$.

§ 3. Extensión algebraica compuesta de un cuerpo

Extensión finita de un cuerpo. Sea $\mathcal{P}$ un sub-cuerpo del cuerpo$\mathcal{F}$. Entonces se puede considerar $\mathcal{F}$como un espacio vectorial sobre $\mathcal{P}$, es decir considerar el espacio vectorial

$\langle F, +, \{\omega_\lambda \mid \lambda \in P\}\rangle$,

dondeω_λ es una operación de multiplicación de los elementos de F por un escalar $\lambda \in P$.

DEFINICIÓN. Una extensión $\mathcal{F}$ del cuerpo $\mathcal{P}$ se denomina finito si $\mathcal{F}$, espacio vectorial sobre $\mathcal{P}$, es de dimensión finita, esta extensión sedenota$[\mathcal{F} : \mathcal{P}]$.

PROPOSICIÓN 3.1. *Si α es un elemento algebraico de grado n sobre $\mathcal{P}$, entonces*$[\mathcal{P}(\alpha) : \mathcal{P}] = n$.

Esta proposición se deriva directamente del TEOREMA 2.5.

DEFINICIÓN. Una extensión $\mathcal{F}$ del cuerpo $\mathcal{P}$ se denomina algebraica si cada elemento de F es algebraico sobre $\mathcal{P}$.

TEOREMA 3.2. *Toda extensión finita $\mathcal{F}$ del cuerpo $\mathcal{P}$ es algebraica sobre $\mathcal{P}$.*

Demostración. Sea n la dimensión de $\mathcal{F}$ sobre $\mathcal{P}$. El TEOREMA es aparentemente verdadero si $n = 0$. Plantéese que $n > 0$. Cualesquiera$n + 1$ elementos de F son linealmente dependientes sobre $\mathcal{P}$. En particular, el sistema de elementos*1, α, . . . ,*α^nes linealmente dependiente, es decir que existe en P elementos $c_0, c_1, \ldots, c_n$ no todos nulos, tales que

$$c_0 \cdot 1 + c_1\alpha + \ldots c_n\alpha^n = 0.$$

Por consiguiente, el elemento α es algebraico sobre $\mathcal{P}$. □

Obsérvese que existen extensiones algebraicas del cuerpo que no son extensiones finitas.

Extensión algebraica compuesta de un cuerpo. Una extensión $\mathcal{F}$ del cuerpo $\mathcal{P}$ se denomina compuesta si existe una cadena ascendente de sub-cuerpo $\mathcal{L}_i$ del cuerpo $\mathcal{F}$, tal que

$$\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_{\mathcal{R}} = \mathcal{F} \text{y} \mathcal{K} > 1.$$

TEOREMA 3.3. *Sea$\mathcal{F}$ una extensión finita del cuerpo $\mathcal{L}$ y $\mathcal{L}$ una extensión finita del cuerpo $\mathcal{P}$. Entonces, $\mathcal{F}$ es una extensión finita del cuerpo $\mathcal{P}$ y*

(I) $[\mathcal{F} : \mathcal{P}] = [\mathcal{F} : \mathcal{L}] \cdot [\mathcal{L} : \mathcal{P}]$.

Demostración. Sean

(1) $\alpha_1, \ldots, \alpha_m$

la base del cuerpo $\mathcal{L}$ sobre $\mathcal{P}$ (considerado como un espacio vectorial) y

(2) $\beta_1, \ldots, \beta_n$

la base del cuerpo $\mathcal{F}$ sobre $\mathcal{L}$. Todo elemento d de F puede expresarse linealmente en función de la base:

(3) $d = l_1\beta_1 + \ldots + l_n\beta_n \qquad (l_{\mathcal{R}} \in P)$.

Los coeficientes $l_{\mathcal{R}}$ pueden expresarse linealmente en función de la base (1):

(4) $l_{\mathcal{R}} = p_{1\mathcal{R}}\alpha_1 + \ldots + p_{m\mathcal{R}}\alpha_m \qquad (p_{i\mathcal{R}} \in P)$.

Al llevar la expresión del coeficiente $l_{\mathcal{R}}$ en (3), se obtiene

$$d = \sum_{\substack{i\in\{1,\ldots,m\} \\ \mathcal{R}\in\{1,\ldots,n\}}} p_{i\mathcal{R}}\,\alpha_i\beta_{\mathcal{R}}.$$

Así, cada elemento del cuerpo $\mathcal{F}$ se representa bajo la forma de una combinación lineal del elemento del conjunto B, donde

$$B = \{\alpha_i\beta_{\mathcal{R}} \mid i \in \{1, \ldots, m\},\ \mathcal{K} \in \{i, \ldots, n\}\}.$$

Nótese que el conjunto B se compone de nm elementos.

Muéstrese que B es la base de $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$. Se debe mostrar que el sistema delos elementos del conjunto B es linealmente independiente. Sea

(5)

$$\sum_{i,\mathcal{R}} c_{i\mathcal{R}}\alpha_i\beta_{\mathcal{R}} = 0,$$

donde$c_{i\mathcal{R}}\alpha_i \in P$. Dado que el sistema (2) es linealmente independiente sobre $\mathcal{L}$, resulta de (5) la igualdad

(6) $c_{1\mathcal{R}}\alpha_1 + \ldots + c_{m\mathcal{R}}\alpha_m = 0 \qquad (\mathcal{K} = 1, \ldots, n)$.

Los elementos $\alpha_1, \ldots, \alpha_m$siendo linealmente independientes sobre $\mathcal{P}$, resulta de (6) las igualdades

$$c_{1\mathcal{R}} = 0, \ldots, c_{m\mathcal{R}} = 0 \qquad (\mathcal{K} = 1, \ldots, n),$$

que muestra que todos los coeficientes en (5) son nulos. Así, el sistema de elementos de B es linealmente independiente y es una base de $\mathcal{F}$ sobre $\mathcal{P}$.

En resumen, se estable que $[\mathcal{F} : \mathcal{P}] = nm = [\mathcal{F} : \mathcal{L}] \cdot [\mathcal{F} : \mathcal{P}]$. Por consiguiente, $\mathcal{F}$ es una extensión finita del cuerpo $\mathcal{P}$ y se tiene la fórmula (I). □

DEFINICIÓN. Una extensión $\mathcal{F}$ del cuerpo $\mathcal{P}$ se llama *extensión algebraica compuesta* si existe una cadena ascendente del sub-cuerpo del cuerpo $\mathcal{P}$

(1) $\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_{\mathcal{R}} = \mathcal{F} \qquad (\mathcal{K} > 1)$

Tal que para $i = 1,\ldots,\mathcal{K}$los cuerpos$\mathcal{L}_i$ son una extensión algebraica simple del cuerpo $\mathcal{L}_{i-1}$. El número $\mathcal{K}$ se denomina *longitud de la cadena* (1).

COROLARIO 3.4. *Una extensión algebraica compuesta $\mathcal{F}$ del cuerpo $\mathcal{P}$ es una extensión finita del cuerpo $\mathcal{P}$.*

La demostración se efectúa fácilmente por inducción sobre la longitud de la cadena (1) que se apoya sobre el TEOREMA 3.3.

TEOREMA 3.5. Sea $\alpha_1,\ldots,\alpha_{\mathcal{R}}$ elementos algebraicos del cuerpo $\mathcal{F}$sobre el cuerpo$\mathcal{P}$. Entonces el cuerpo $\mathcal{P}(\alpha_1,\ldots,\alpha_{\mathcal{R}})$ es una extensión finita del cuerpo $\mathcal{P}$.

Demostración. Sea

$\mathcal{L}_0 = \mathcal{P},\ \mathcal{L}_1 = \mathcal{P}[\alpha_1],\ \mathcal{L}_2 = \mathcal{P}[\alpha_1,\ \alpha_2],\ldots,\mathcal{L}_{\mathcal{R}} = \mathcal{P}[\alpha_1,\ldots,\alpha_{\mathcal{R}}]$.

En este caso $\mathcal{L}_1 = \mathcal{P}[\alpha_1]$ es una extensión algebraica simple del cuerpo $\mathcal{L}_0$; $\mathcal{L}_2$ es una extensión algebraica simple del cuerpo $\mathcal{L}_1$, puesto que

$\mathcal{L}_2 = \mathcal{P}[\alpha_1,\ \alpha_2] = (\mathcal{P}[\alpha_1])[\alpha_2] = \mathcal{L}_1[\alpha_2] = \mathcal{L}_1(\alpha_2)$, etc.

Así,

$\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_{\mathcal{R}} = \mathcal{F}$,

donde$\mathcal{L}_i = \mathcal{L}_{i-1}(\alpha_i)$ para $i = 1,\ldots,\mathcal{K}$, es decir que cada término de la cadena (2) es una extensión algebraica simple del término precedente de la cadena, en resumen, el cuerpo $\mathcal{F}$ es una extensión algebraica compuesta del cuerpo $\mathcal{P}$. Por consiguiente, en virtud del corolario 3.4, el cuerpo $\mathcal{F}$ es una extensión finita del cuerpo $\mathcal{P}$. □

COROLARIO 3.6. *Una extensión algebraica compuesta de un cuerpo es una extensión algebraica de ese cuerpo.*

Simplicidad de la extensión algebraica compuesta de un cuerpo.

TEOREMA 3.7. *Supóngase que un cuerpo numérico $\mathcal{F}$ es una extensión algebraica compuesta del cuerpo $\mathcal{P}$.*Entonces $\mathcal{F}$ es una extensión algebraica simple del cuerpo $\mathcal{P}$.

Demostración. Sea $\mathcal{P} \subset \mathcal{L} \subset \mathcal{F}$, con $L = P(\alpha)$, $F = L(\beta)$ y por consiguiente,

$F = P(\alpha,\beta)$.

Sean f y g polinomios mínimos sobre $\mathcal{P}$ respectivamente para los números α y β y $\operatorname{grad} f = m$, $\operatorname{grad} g = n$. Los polinomios f y g son irreducibles sobre $\mathcal{P}$ y, por consiguiente, no poseen en el cuerpo $\mathcal{C}$ números complejos de las raíces múltiples. Sean

$\alpha = \alpha_1,\ldots,\alpha_m$raíces del polinomio f en **C**y

$\beta = \beta_1,\ldots,\beta_n$raíces del polinomio g en **C.**

Considérese el conjunto finito M:

$$M = \left\{\frac{\alpha_i - \alpha}{\beta - \beta_{\mathcal{R}}} \mid i \in \{1,\ldots,m\},\quad \mathcal{K} \in \{2,\ldots,n\}\right\}.$$

Como $\mathcal{P}$ es un conjunto numérico (y, como consecuencia, infinito) existe en P un número c distinto de los elementos del conjunto M $c \in P \setminus M$, $c \notin M$. Sea

(1) $\gamma = \alpha + c\beta$.

Se tiene entonces las relaciones

(2) $\gamma \neq \alpha_i + c\beta_{\mathcal{R}} \qquad (i \in \{1,\ldots,m\},\quad \mathcal{K} \in \{2,\ldots,n\})$.

En efecto, en caso de igualdad de $\alpha + c\beta = \alpha + c\beta_{\mathcal{R}}$, se tendría

$$c = \frac{\alpha_i - \alpha}{\beta - \beta_{\mathcal{R}}} \in M,$$

lo que es contradictorio a la elección del número c.

Sean $\mathcal{F}_1 = \mathcal{P}(\gamma)$ y $\mathcal{F}_1[x]$ un anillo de los polinomios en x.

Supóngase que $h = f(\gamma - cx)$ es un polinomio de $F_1[x](\gamma,\ c \in P(\gamma) = \mathcal{F}_1)$. Muéstrese que $x - \beta$es el máximo común divisor de los polinomios h y g en el anillo $\mathcal{F}_1[x]$. Dado que $g(\beta) = 0$, $x - \beta$ divide ag en $\mathcal{C}[x]$. Luego, en virtud de (1)

$$h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0.$$

Así pues, $x - \beta$ divide el polinomio h y g en el anillo $\mathcal{C}[x]$. Así $x - \beta$ es un divisor común de h y g en el anillo $\mathcal{C}[x]$.

Demuéstrese que g y h no tienen en $\mathcal{C}$ raíces distintas de β. En efecto, plantéese que $\beta_{\mathcal{R}}, \mathcal{K} \in \{2,\ldots,n\}$ es su raíz común. Entonces, $h(\beta_{\mathcal{R}}) = f(\gamma - \beta_{\mathcal{R}}) = 0$. Se encontrará pues un índice $i \in \{1,\ldots,m\}$ para el cual $\gamma = \alpha_i + c\beta_{\mathcal{R}}(\mathcal{K} > 1)$, o está en contradicción con (2). Al apoyarse sobre lo que precede se concluye que $x - \beta$ es el máximo común divisor de g y h en $\mathcal{C}[x]$.

Dado que $x - \beta$ es un polinomio mónico, resulta que $x - \beta$ es el máximo común divisor de g y h en el anillo $\mathcal{F}_1[x]$. Así pues,

$$(x - \beta) \in F_1[x] \text{y} \beta \in F_1 = P(\gamma).$$

Además, $\alpha = \gamma - c\beta \in F_1$. Así,

$$F = P(\alpha, \beta) \subset F_1, \qquad F_1 \subset F.$$

Así pues, $F = P(\gamma)$. Dado que γ(por otra parte cualquier elemento de F) es un elemento algebraico sobre $\mathcal{P}$ y, se tieneque $\mathcal{F} = \mathcal{P}(\gamma)$es la extensión algebraica simple buscada del cuerpo $\mathcal{P}$. □

Cuerpo de números algebraicos. En la clase de los sub-cuerpos de un cuerpo de los números complejos el cuerpo de los números algebraicos es uno de los más importantes.

DEFINICIÓN. Se denomina *número algebraico* a un número complejo que constituye una raíz de un polinomio de grado positivo con coeficientes racionales.

Nótese que un número algebraico es un número complejo cualquiera algebraico sobre el cuerpo Q. En particular todo número racional es algebraico.

TEOREMA 3.8. *El conjunto A de todos los números algebraicos se encierran en el anillo $\mathcal{C} = \langle \boldsymbol{C}, +, -, \cdot, 1\rangle$de los números complejos.*

Demostración. Sean a y b todos elementos de A. Según el corolario 3.6, el cuerpo $Q(a, b)$ es algebraico sobre Q.Por lo tanto los números $a + b, -a, ab, 1$son números algebraicos, es decir pertenecen al conjunto A. El conjunto Aes cerrado respecto a las operaciones principales del anillo $\mathcal{C}$. El algebra $\mathcal{A}$ es pues un anillo como sub-anillo del anillo $\mathcal{C}$.

Además, si α es un elemento no nulo de A, se tienen $\alpha^{-1} \in \mathbf{Q}(a, b)$ y, por lo tanto, pertenece a A. Por consiguiente, el algebra $\mathcal{A}$ es un cuerpo, un sub-cuerpo del cuerpo $\mathcal{C}$. □

DEFINICIÓN. *El cuerpo $\mathcal{A} = \langle A, +, -, \cdot, 1\rangle$ se denomida cuerpo de los números algebraicos.*

Cierre algebraico de un cuerpo de los números algebraicos.

TEOREMA 3.9 *Un cuerpo de los números algebraicos es algebraicamente cerrado.*

Demostración. Sea $\mathcal{A}[x]$ un anillo de polinomios en x sobre el cuerpo $\mathcal{A}$ de los números algebraicos. Sea

$f = a_0 + a_1x + \ldots + a_nx^n \qquad (a_0, \ldots, a_n \in A)$

un polinomio cualquiera del grado positivo de $A[x]$. Se demuestra que f admite una raíz en A. Dado que $f \in \boldsymbol{C}[x]$ y que el cuerpo $\mathcal{C}$ es algebraicamente cerrado, f admite una raíz en $\mathcal{C}$, es decir existe un numero complejo $c$tal que$f(c) = 0$. Sean $\mathcal{L} = Q(a_o, \ldots, a_n)$ y $\mathcal{L}(c)$ una extensión algebraica simple del cuerpo $\mathcal{L}$ por añadidura de c. Entonces, $Q \overset{-3}{} \mathcal{L} \overset{-3}{} \mathcal{L}(c)$,$\mathcal{L}(c)$ siendo la extensión finita del cuerpo $\mathcal{L}$. En virtud del TEOREMA 3.2, $\mathcal{L}$ es una extensión finita del cuerpo Q. En virtud del TEOREMA 3.3, $\mathcal{L}(c)$ es una extensión finita del cuerpo Q. De donde, según el TEOREMA 3.2, el cuerpo $\mathcal{L}(c)$ es pues una extensión algebraica del cuerpo Q y, por consiguiente, $c \in A$. Así cualquier polinomio de $A[x]$ de grado positivo admite en A una raíz, es decir el cuerpo $\mathcal{A}$ es algebraicamente cerrado. □

Ejercicios

1. Buscar el grado del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$ si
   (a) $\mathcal{F} = Q(\sqrt{2}, \sqrt{3}), \quad \mathcal{P} = Q$; b) $\mathcal{F} = Q(\sqrt{2}, \sqrt[3]{5}), \quad \mathcal{P} = Q(\sqrt{2})$; c) $\mathcal{F} = \mathcal{R}, \quad \mathcal{P} = \mathcal{R}$.
2. Buscar la base y el grado del cuerpo $\mathcal{F}$ sobre el cuerpo $\mathcal{P}$ si
   (a) $\mathcal{F} = Q(i, \sqrt[3]{2}), \mathcal{P} = Q$; b) $\mathcal{F} = \mathcal{R}(-i), \mathcal{P} = \mathcal{R}$; c) $\mathcal{F} = \mathcal{C}, \quad \mathcal{P} = \mathcal{C}$.
3. Sean f y g polinomios sobre el cuerpo de los números racionales que admite una raíz real común. Demostrar que f y g poseen un divisor común de potencia positiva con coeficientes racionales.
4. Demostrar que un polinomio irreducible sobre un cuerpo numérico no admite raíces múltiples en un cuerpo de los números complejos.
5. Demostrar que un número complejo es un número algebraico si y sólo si es una raíz de un polinomio de grado positivo con coeficientes enteros.

§ 4.Condiciones de resolubilidad de una ecuación de tercer grado por radicales cuadrados

Noción de resolubilidad de una ecuación por radicales cuadrados.

DEFINICIÓN. *Un cuerpo $\mathcal{F}$ se denomina extensión cuadrática del cuerpo $\mathcal{P}$ si existe un elemento αtal que*$F = P(\alpha), \alpha \notin P, \alpha^2 \in P$.

Ejemplos. 1. El cuerpo $Q(2^{1/2})$ es una extensión cuadrática del cuerpo Q.

2. El cuerpo $\mathcal{R}(i)$ es una extensión cuadrática del cuerpo $\mathcal{R}$.

3. El cuerpo $Q(2^{1/3})$ no es una extensión cuadrática de Q.

Se dice que la ecuación

(1) $x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \quad (a_i \in \mathbf{Q})$

Es resoluble por radicales cuadrados si sus raíces pueden expresarse de manera racional (es decir con la ayuda de las operaciones de adición, sustracción, multiplicación y división) por raíces de una cadena de ecuaciones cuadrática binomiales:

$x^2 - \alpha_0 = 0, \ \alpha_0 \in \mathbf{Q} = F_0;$
$x^2 - \alpha_1 = 0, \ \alpha_1 \in F_1 = F_0(\sqrt{\alpha_0});$
$x^2 - \alpha_2 = 0, \ \alpha_2 \in F_2 = F_1(\sqrt{\alpha_1});$
. . . . . .

$$x^2 - \alpha_{\mathcal{R}-1} = 0, \qquad \alpha_{\mathcal{R}-1} \in F_{\mathcal{R}-1} = F_{\mathcal{R}-2}\left(\sqrt{\alpha_{\mathcal{R}-2}}\right).$$

Así, todas las raíces de la ecuación (1) se expresan de forma racional por los números $\sqrt{\alpha_0}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{\mathcal{R}-1}}$ y pertenecen al cuerpo $F_{\mathcal{R}} = F_{\mathcal{R}-1}\left(\sqrt{\alpha_{\mathcal{R}-1}}\right)$.

En otras palabras, la ecuación (1) es resoluble por radicales cuadrados si existe una cadena ascendente de los cuerpos numéricos

$$Q = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \ldots \subset F_{\mathcal{R}-1} \subset F_{\mathcal{R}}$$

tal que cada cuerpo F_i de la cadena sea una extension cuadrática del cuerpo prescedente F_{i-1}, el cuerpo $F_{\mathcal{R}}$que contiene todas las raices de la euación (1).

DEFINICIÓN. Se dice que la ecuación (1) es resoluble por radicales si sus raices pueden expresarse de manera racional por raices de una cadena de ecuaciones binomiales:

$$\begin{aligned}
&x^{n0} - \alpha_0 = 0, && \alpha_0 \in \mathbf{Q} = F_0;\\
&x^{n1} - \alpha_1 = 0, && \alpha_1 \in F_1 = F_0\left(\sqrt[n0]{\alpha_0}\right);\\
&x^{n2} - \alpha_2 = 0, && \alpha_2 \in F_2 = F_1\left(\sqrt[n1]{\alpha_1}\right);\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x^{n\mathcal{R}-1} - \alpha_{\mathcal{R}-1} = 0, && \alpha_{\mathcal{R}-1} \in F_{\mathcal{R}-1} = F_{\mathcal{R}-2}\left(\sqrt[n\mathcal{R}-2]{\alpha_{\mathcal{R}-2}}\right).
\end{aligned}$$

Así, todas las raíces de la ecuación (1) se expresan de manera racional por los números $\sqrt[n0]{\alpha_0}, \ldots, \sqrt[n\mathcal{R}-1]{\alpha_{\mathcal{R}-1}}$ y pertenecen al cuerpo $F_{\mathcal{R}} = F_{\mathcal{R}-1}\left(\sqrt[n\mathcal{R}-1]{\alpha_{\mathcal{R}-1}}\right)$.

Condiciones de resolubilidad de una ecuación de tercer grado por radicales cuadrados.

TEOREMA 4.1. *Una ecuación de tercer grado*

(1) $x^3 + ax^2 + bx + c = 0$

con coeficientes racionales es resoluble por radicales cuadrados si y sólo si admite al menos una raíz racional.

Demostración. Si el polinomio $f = x^3 + ax^2 + bx + c$ admite al menos una raíz racional, por ejemplo d, entonceseste polinomio puede representarse bajo la forma

$$f = (x - d)(x^3 + ex + g),$$

Donde $e, g \in \mathbf{Q}$. La ecuación (1) es pues resoluble por radicales cuadrados.

Supóngase que la ecuación (1) es resoluble por radicales cuadrados mientras no admita raíces racionales. Existe entonces una cadena de extensiones cuadráticas

(2) $\mathbf{Q} = F_0 \subset F_1 \subset \ldots \subset F_{\mathcal{R}-1} \subset F_{\mathcal{R}}$,

tal como por lo menos una de las raíces x_1, x_2, x_3 de la ecuación (1) este contenida en $F_{\mathcal{R}} \setminus F_{\mathcal{R}-1}$, por ejemplo

(3) $x_1 \in F_{\mathcal{R}} \setminus F_{\mathcal{R}-1}$,

y ninguna de las raíces $x_1,\ x_2,\ x_3$ de la ecuación (1) no se contiene en $F_{\mathcal{R}-1}$,

(4) $\{x_1,\ x_2,\ x_3\} \cap F_{\mathcal{R}-1} = \emptyset$.

El cuerpo $F_{\mathcal{R}}$ es una extensión cuadrática del cuerpo $F_{\mathcal{R}-1}$, es decir que existe un elemento $\alpha \in F_{\mathcal{R}} \setminus F_{\mathcal{R}-1}$tal que

(5) $F_{\mathcal{R}} = F_{\mathcal{R}-1}(\alpha), \qquad \alpha \notin F_{\mathcal{R}-1}, \qquad \alpha^2 \in F_{\mathcal{R}-1}$.

En base a (3) y (5), se concluye que

(6) $x_1 = p + q\alpha$, donde $p, q \in F_{\mathcal{R}-1}, \qquad q \neq 0$.

Una verificación directa muestra que $p - q\alpha$ es igualmente una raíz del polinomio f. En efecto,

(7) $f\left(p - q\alpha\right) = \left(p - q\alpha\right)^3 + a\left(p - q\alpha\right)^2 + b\left(p - q\alpha\right) + c = A + B\alpha$,

donde

(8)
$$A = f(p) + 3pq^2\alpha^2 + aq^2\alpha^2,$$
$$B = 3p^2q + q^3\alpha^2 + 2apq + bq.$$

Dado que $A, B \in F_{\mathcal{R}-1}$ y $\alpha \notin F_{\mathcal{R}-1}$, resulta de

(9) $f\left(p - q\alpha\right) = A + B\alpha = 0$

que

(10)$A = B = 0$.

En base a (7), (8) (9) y (10), se concluye que

$$f\left(p - q\alpha\right) = A - B\alpha = 0.$$

Así, $p - q\alpha$ es igualmente una raíz del polinomio f. Sea $x_2 = p - q\alpha$. Entonces, en virtud de (6), $x_1 - x_2 = 2q\alpha \neq 0$ y, por consiguiente, $x_1 \neq x_2$.

Según las fórmulas de Viète, $x_1 + x_2 + x_3 = -a$. Además, en virtud de (6), $x_1 + x_2 = 2p \in F_{\mathcal{R}-1}$.Así pues, $x_3 = -a - 2p \in F_{\mathcal{R}-1}$,lo que contradice a la proposición (4). □

COROLARIO 4.2. La ecuación (1) con coeficientes racionales es resoluble por radicales cuadrados si y sólo si el polinomio $x_3 + ax_2 + bx + c$ es irreducible en el anillo $Q[x]$.

Ejemplos de problemas irresolubles por radicales cuadrados. Se demuestra en geometría que las raíces de la ecuación $x_3 + ax_2 + bx + c = 0$ con coeficientes racionales pueden construirse con regla y compás si y sólo si esta ecuación es resoluble por radicales cuadrados, es decir si la solución de esta ecuación se reduce al de una cadena de ecuaciones cuadráticas.

Problema de la duplicación del cubo. *Construir la arista de un cubo cuyo volumen es el doble al del cubo dado.*

Se dispone solamente de un segmento: la arista del cubo dado: plantéese que este segmento es un segmento unitario. Entonces, la longitud x de la arista del cubo debe verificar la ecuación

(1) $x_3 = -2 = 0.$

Esta ecuación es irresoluble por radicales cuadrados, puesto que no posee raíces racionales. Por tanto, las raíces de la ecuación (1) no pueden construirse con regla y compás.

Problema de trisección de un ángulo. Dividir el ángulo dado tres partes iguales.

Puede imaginarse dos rayos de origen O formando un ángulo φ. Trácese un arco de círculo de radiounitario. Constrúyase el punto A de manera que el segmento OA tuviera una longitud $a = \cos\varphi$. Recíprocamente: al conocer el segmento OA de longitud $\cos\varphi$ es fácil de construir el ángulo por medio de regla y compás. Se puede considerar que el ángulo x $\frac{\varphi}{3}$ el que se busca. Como

$$\cos\varphi + i\ \mathrm{sen}\,\varphi = \left(\cos x\ \frac{\varphi}{3} + i\ \mathrm{sen}\frac{\varphi}{3}\right)^3 = \cos^3\frac{\varphi}{3} - 3\ \cos\frac{\varphi}{3}\mathrm{sen}^2\frac{\varphi}{3} + i\left(3\cos^2\frac{\varphi}{3}\mathrm{sen}\frac{\varphi}{3} - \mathrm{sen}^3\frac{\varphi}{3}\right),$$

se tiene

$$\cos\varphi = \cos^3\frac{\varphi}{3} - 3\ \cos\frac{\varphi}{3}\mathrm{sen}^2\frac{\varphi}{3} = \cos^3\frac{\varphi}{3} - 3\left(1 - \cos^2\frac{\varphi}{3}\right)$$

y

$$4\ \cos^3\frac{\varphi}{3} - 3\ \cos\frac{\varphi}{3} - \cos\varphi = 0.$$

Como $x = \frac{\varphi}{3}$, se tiene

(1) $4x^3 - 3x - a = 0.$

Para $\varphi = \frac{\pi}{2}, a = 0$ y, por lo tanto, la ecuación (1) es resoluble por radicales cuadrados.

Pero si $\varphi = \frac{\pi}{2}$, $a = \cos\frac{\pi}{2} = \frac{1}{2}$, y resulta la ecuación

(1) $8x^3\ 6x - 1 = 0.$

Al plantearlo en$y = 2x$, se obtiene

(2) $y - 3y - 1 = 0.$

La ecuación (3) y, por lo tanto, (2) es irresoluble por radicales cuadrados, puesto que no tiene raíces racionales. Por consiguiente, las raíces de estas ecuaciones no pueden construirse con regla y compás. Así la trisección del ángulo π / 3con regla ycompás es imposible.

Problema de construcción de un heptágono regular. Construir un heptágono regular inscrito en un círculo unitario.

Las raíces de la ecuación $z^7 - 1 = 0$representanpor los vértices de un heptágono regularinscrito en un círculo unitario. Una de las raíces de esta ecuación es la unidad, en cuanto a las otras, verifican la ecuación

(1) $z^6 + z^5 + z^4 + z^3 + z^2 + z = 0.$

Demuéstrese que la ecuación (1) es irresoluble por radicales cuadrados. Al dividir los dos miembros de la ecuación (1) por z^3 y al agrupar los términos, resulta

$\left(z + \frac{1}{z}\right)^3 - 3\left(z + \frac{1}{z}\right) + \left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0.$

Al plantear

(2) $t = z + \frac{1}{z},$

se obtiene

(3) $t^3 + t^2 - 2t - 1 = 0.$

La ecuación (3) es irresoluble por radicales cuadrados, puesto que no tiene raíces racionales. La ecuación (1) es pues irresoluble por radicales cuadrados. En efecto, si la ecuación (1) fuese resoluble por radicales cuadrados, entonces, en virtud de (2), la ecuación (3) sería también resoluble por radicales cuadrados. Por consiguiente, las raíces de la ecuación (1) no pueden construirse al compás y con regla. Se deduce que *un heptágono regular no puede construirse al compás y con regl*a.

¿Para cuales n naturales $(n > 2)$ pueden construir un polígono regular en n ángulos mediante un compás y con regla?

En 1796, Gauss resolvió completamente este problema. Gauss demostró que la construcción es posible solamente en el caso donde n puede representarse bajo la forma

$$n = 2^{\mathcal{R}} p_1 p_2 \ldots p_m,$$

Donde k es un número natural y $p_1, \ldots, p_m$ son números primos diferentes de la forma $2^m + 1$ $(m \in \mathbf{N} \setminus \{0\})$.

Ejercicios

1. Mostrar que el polinomio $x^6 + x^3 + 1$ es irreducible sobre el cuerpo de los números racionales.

2. Mostrar que un polinomio de tercer grado sobre un cuerpo eso bien irreducible o bien admite una raíz de este cuerpo. ¿El polinomio $x^5 - 5x^2 + 1$ es irreducible sobre el cuerpo de los números racionales?
3. Mostrar que el polinomio con dos variables $x^2 + y^2 - 1$ es irreducible sobre el cuerpo de los números racionales. ¿es irreducible sobre el cuerpo de los números complejos?
4. Demostrar que la ecuación $x^5 - 1 = 0$ es resoluble por radicales cuadrados.
5. Demostrar que un pentágono regular puede construirse con regla y compás.
6. Demostrar que un eneágono regular no puede construirse con regla y compás.

ÍNDICE